

13 June 2014

Missile Defense Agency Assurance Provisions (MAP)



Distribution D: Distribution Authorized to the Department of Defense and U.S. DOD Contractors only for the purpose of contract performance, an arrangement requiring that this information be held in confidence, and that public distribution is restricted. Other requests shall be referred to MDA/DAC Contracting Office.

For Official Use Only Statement: This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the Freedom Of Information Act (5 U.S.C. Section 552). Exemptions (3) & (5) apply.

Warning: This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. section 2751 et. seq.) or the Export Administration Act of 1979, as amended (50 U.S.C Appendix 2401 et. seq.) Violation of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DOD directive 5230.25

Destruction Statement: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

~~For Official Use Only~~

Hard copies of this document are for REFERENCE ONLY and shall not be considered the latest revision.

13 June 2014

MDA-QS-001-MAP-Rev B

~~For Official Use Only~~

Missile Defense Agency Assurance Provisions (MAP)


APPROVED BY:



Date: 23 MAY 2014

MIKE WADZINSKI
Director
Quality, Safety, and Mission Assurance

APPROVED BY:



Date: 6/13/2014

J. D. SYRING
Vice Admiral, USN
Director

13 June 2014

MDA-QS-001-MAP-Rev B

~~For Official Use Only~~

Revision Record

Revision	Date	Change	Affected Pages
Original	9 January 2004	Reflects CCB approval with comments	
Rev A	28 November 2006	Addressed IG Audit Findings and MDA Reengineering	All
Rev B	13 June 2014	Incorporates updates and MDA community comments Added Preface Added Appendix A, Requirements Applicability Matrix Added Appendix B, MDA Core Metrics Added Appendix C, Workmanship Requirements Added Appendix D, Acronyms Added Appendix E, Definitions	All

13 June 2014

MDA-QS-001-MAP-Rev B

~~For Official Use Only~~

PREFACE

In 2002, the Quality, Safety, and Mission Assurance Directorate (QS) was established as the independent organization within the Missile Defense Agency responsible for establishing and maintaining quality, safety and mission assurance (QSMA) policy and requirements across a wide range of evolving development and legacy programs. The Agency Director, Lt. General Kadish, was seeking a solution for test failures within the programs caused by what he referred to as quality control problems. The new QS Director had a vision to create a policy document that would integrate best practice disciplines of design assurance, mission assurance, quality assurance, and safety into a single volume of requirements; MDA Assurance Provisions (MAP). The document's scope was limited to only safety and mission critical items (hardware and software). A small team was assigned and dedicated to writing the requirements based on other successful programs, like the Navy's Trident and STANDARD Missile Programs, NASA, and Air Force Space and Missile Systems Center; academia, Defense Acquisition University; and history, Military and Industry Standards, lessons learned, and common sense. The challenge was to create a document that would encompass all aspects of planning, design, development, fabrication, test, deployment, and support in an evolutionary acquisition environment primarily focused on development but desiring a production focus and discipline.

The MAP challenge was the same as the Agency challenge to bring process rigor into a development environment and reverse the trend of test flight failure, create a quality environment, and institutionalize a quality culture for team success. The original MAP drafts were vetted first through the QSMA community and then through a combined industry and element team. The MAP was revised based on these vetting comments and submitted for review and comment from all MDA elements. Like the current process, comments were adjudicated and discussed; the MAP was revised and discussed, and finally signed by then Director on 4 January 2004.

The challenge was far from over. The question remained on how to adapt and scale the MAP to each program based on product complexity, life cycle phase, and existing legacy contracts written in an acquisition reform language. Some programs felt that the MAP was in conflict with the Acquisition Reform Movement, but the requirements were deemed necessary to focus on attention to detail. In defense of the MAP, QS cited a RAND study which found that the drastic measures taken during acquisition reform should not apply equally to all programs. The RAND report stated that acquisition reform was more successful in high volume, low technology programs (bombs and bullets) but unsuccessful in low production, advanced technology programs (missiles and sensors). The original concept for MAP on contract was the Mission Assurance Implementation Plan (MAIP). Each program was to develop an implementation matrix to indicate how each requirement would be met, modified, or omitted based on product complexity, life cycle phase, current program or contractor procedure, but mostly by the reality of current contract requirements. The MAP requirements and MAIP process were moderately successful introducing a new set of requirements and quality focus into programs and prime contractors. The greatest challenge was driving the requirements beyond the primes to the supply chain where quality is most important and needed as evidenced by test failures traced to supplied items and a lapse in quality.

In November 2006 MAP Revision A was approved by the Director. Revision A incorporated lessons learned from experience with the previous revision, recommendations from a DOD Inspector General (IG) review, and MDA reengineering directives. Of these three change factors, the most significant was the incorporation of the DOD IG review recommendations to address the Bob Stump National Defense Authorization Act concerning acquisition and support of safety and mission critical software and firmware.

As the Agency meets the challenges of inserting new technology to counter evolving threats, the focus must remain on quality and attention to detail. Revision B of the MAP presents an opportunity to incorporate more lessons learned and new ideas to meet the challenge. The future success of the MAP lies in the proposed Revision B and the opportunity afforded by new contracts for existing programs. The MAP Revision B is revised based on more than eight years of lessons learned, field experience, and results from years of QSMA audits. The proposed revision is tailorable through the Requirements

Applicability Matrix to allow for program complexity, life cycle phase, and existing processes with a track record of yielding quality products and services. The expectation is that the MAP and its requirements will be flowed down the supply chain where the improvement in process rigor and quality improvement is most needed. The MAP remains true to the original vision of a single document that provides a measurable, standardized set of Quality, Safety, and Mission Assurance requirements that Government and contractors apply to safety and mission critical items in support of evolutionary acquisition and deployment of MDA systems.

Table of Contents

PREFACE	i
1.0 SCOPE.....	1
1.1 Purpose	1
1.2 Applicability and Accountability.....	1
1.2.1 Mission Assurance Implementation Plan	1
1.2.2 MAP on Contract	1
1.3 International Traffic in Arms Regulations	1
1.4 Order of Precedence.....	2
2.0 APPLICABLE DOCUMENTS.....	3
3.0 QUALITY, SAFETY, AND MISSION ASSURANCE PROVISIONS	9
3.1 Management	9
3.1.1 Contract Reviews	9
3.1.2 Management Reviews.....	10
3.1.3 Technology Change Management.....	10
3.1.4 Process Improvements and Core Metrics.....	10
3.1.4.1 MDA Core Metrics	10
3.1.5 Integrated Digital Environment.....	11
3.1.6 Risk Management Program	12
3.1.6.1 Risk Management Plan.....	13
3.1.7 Pedigree Program	13
3.1.8 Internal Evaluation Program.....	14
3.1.9 Training and Certification Program	14
3.1.9.1 Training	14
3.1.9.2 Certification.....	15
3.1.10 Problem and Failure Reporting and Corrective Action System	15
3.1.11 Data Exchange Programs Participation	15
3.1.12 MDA Insight and Oversight	16
3.1.12.1 MDA Assurance Representatives.....	16
3.1.12.2 MDA Inspections.....	16
3.1.12.3 MDA Evaluations	17
3.1.13 Program Reviews.....	17
3.1.14 Government Furnished Material, Equipment, or Information	17
3.1.14.1 Contractor Acquired Property	18
3.1.15 Repair, Refurbishment, and Modification.....	18
3.1.16 Responsible Engineer	18
3.2 Design and Development	19
3.2.1 Integrated Product and Process Development	19
3.2.2 Peer Reviews	19
3.2.3 Technical Performance Measurement	19
3.2.4 Systems Engineering for Design.....	20
3.2.4.1 Element Systems Engineering Plan and Systems Engineering Management Plan.....	20

3.2.4.2	Contractor Systems Engineering Management Plan.....	20
3.2.5	Design for Interoperability	22
3.2.6	Design for Producibility	22
3.2.7	Design for Testability.....	22
3.2.7.1	Testability Program Plan.....	23
3.2.8	Design for Supportability.....	23
3.2.9	Design for Commercial and Non-Developmental Items.....	24
3.2.9.1	COTS/NDI Design Strategies	24
3.2.10	Requirements Traceability and Verification Matrix.....	25
3.2.11	System Design Verification and Validation	25
3.2.12	Safety and Environmental Requirements	26
3.2.13	Open Systems Design and Standards	26
3.2.14	Modeling and Simulation.....	26
3.2.14.1	Verification, Validation, and Accreditation Processes	26
3.2.14.2	Models and Simulations Verification & Validation	27
3.2.14.3	Models and Simulations Accreditation.....	27
3.2.14.4	Accreditation Decision	28
3.2.14.5	Verification, Validation, and Accreditation Documentation.....	28
3.2.15	Classification of Characteristics	28
3.2.15.1	Classification of Characteristics Levels	28
3.2.16	Electromagnetic Environmental Effects Design and Verification	29
3.2.17	Space Radiation, Nuclear Hardness and Survivability Program.....	29
3.2.18	Transition to Operations or Production	29
3.2.18.1	Transition to Production Plan.....	30
3.2.19	Legacy Designs.....	30
3.2.20	BMDs Technical Core Standards	30
3.2.21	Safety and Mission Critical Computing Systems	30
3.2.21.1	Computer System Synchronization	30
3.2.21.2	Read-Only Memories.....	31
3.2.21.3	Self-Checking Design Requirements.....	31
3.2.21.3.1	Time Constraints for Execution	31
3.2.21.3.2	Memory Checks	31
3.2.21.4	Systems Degradation	31
3.2.21.5	Unauthorized Interaction.....	31
3.2.21.6	Unauthorized Access.....	31
3.2.21.7	Peak Load Requirements	32
3.2.21.8	Fault Tolerance	32
3.3	Software and Firmware.....	33
3.3.1	Management Processes	33
3.3.1.1	Intergroup Coordination	33
3.3.1.2	Software Development Plan	33
3.3.1.3	Estimation	34
3.3.1.4	Software and Firmware Risk Management	34
3.3.1.5	Software Process Improvement.....	35
3.3.1.6	Software and Firmware Supplier Management	35
3.3.1.6.1	Flow Down of Requirements	35
3.3.1.6.2	Acceptance of Supplier Software and Firmware Products	35
3.3.1.7	Software Personnel Training	36
3.3.2	Software Development, Maintenance, and Operational Processes	36
3.3.2.1	Requirements.....	36
3.3.2.1.1	Software Reuse.....	37
3.3.2.2	Software Design.....	37
3.3.2.3	Software Code/Implementation	38
3.3.2.3.1	Software Programming Standards.....	38
3.3.2.3.2	Software Coding Standards	39

3.3.2.3.3	Software Code Analysis	40
3.3.2.4	Software Test Coverage and Analysis	41
3.3.2.4.1	Requirements Based Test Coverage Analysis	42
3.3.2.4.2	Structural Test Coverage Analysis.....	42
3.3.2.4.3	Software Threading and Concurrency Analysis.....	42
3.3.2.4.4	Multitasking and Multicore Processing Analysis	42
3.3.2.5	Software Unit Testing	42
3.3.2.6	Software Integration Testing.....	43
3.3.2.7	Software Qualification.....	43
3.3.2.7.1	Software Qualification Test Report	44
3.3.2.7.2	Software Requalification	44
3.3.2.8	Regression Tests	45
3.3.2.9	Software Test Program Status Reports.....	45
3.3.2.10	System Integration.....	45
3.3.2.11	System Qualification	46
3.3.2.12	Software Installation	46
3.3.2.12.1	Software Deliverable Package	46
3.3.2.12.2	Software Release Review	47
3.3.2.13	Software Acceptance.....	47
3.3.2.14	Operation	47
3.3.2.15	Software Maintenance	48
3.3.2.16	Software Retirement	48
3.3.3	Supporting Activities and Processes.....	48
3.3.3.1	Software Quality Assurance Plan	48
3.3.3.2	Software Verification	49
3.3.3.3	Software Validation	49
3.3.3.4	Support of Independent Verification and Validation	50
3.3.3.5	Independent Verification and Validation	51
3.3.3.6	Software Reviews	51
3.3.3.7	Software Audits.....	51
3.3.3.8	Software Problem Reporting.....	52
3.3.3.9	Software Dependability	52
3.3.3.9.1	Software Reliability Program.....	52
3.3.3.9.1.1	Software Reliability Program Plan	52
3.3.3.9.1.2	Software Reliability Documentation.....	53
3.3.3.9.1.3	Allocation of Reliability Requirements to Software.....	53
3.3.3.9.1.4	Software Reliability Analysis.....	53
3.3.3.9.1.5	Software Reliability Evaluation and Achievement	53
3.3.3.9.1.6	Fault Avoidance and Fault Tolerance.....	54
3.3.3.10	Software Safety.....	54
3.3.3.11	Software and Firmware Configuration Management.....	54
3.3.3.11.1	Software Configuration Items.....	54
3.3.3.11.2	Software and Firmware Change Control Process.....	55
3.3.3.11.3	Software Library	55
3.3.3.11.4	Software Configuration Audits.....	55
3.3.3.11.5	Software Status Accounting	56
3.3.3.11.6	Software and Firmware Media Generation	56
3.3.3.12	Software Documentation	56
3.3.4	Firmware Development Plan.....	56
3.4	Technical and Mission Assurance Reviews.....	59
3.4.1	Technical Reviews	59
3.4.1.1	Initial Technical Review	59
3.4.1.2	Alternative Systems Review	60
3.4.1.3	Systems Requirements Review.....	60
3.4.1.4	System Functional Review	60

3.4.1.5	Software Specification Review	60
3.4.1.6	Preliminary Design Assessments/Critical Design Assessments	61
3.4.1.7	Preliminary Design Review	62
3.4.1.8	Critical Design Review	62
3.4.1.9	Test Readiness Review	63
3.4.1.9.1	MDA Executive Level Test Reviews	64
3.4.1.10	System Verification Review	64
3.4.1.11	Functional Configuration Audit	64
3.4.1.12	Production Readiness Review	65
3.4.1.12.1	Follow On Production Readiness Review	66
3.4.1.13	Physical Configuration Audit	66
3.4.2	Mission Assurance Reviews	67
3.4.2.1	Mission Readiness Review	67
3.4.2.2	Pre-Environmental Review	67
3.4.2.3	Pre-Shipment Review	67
3.4.2.4	Mission Operations Review	68
3.4.2.5	Flight Operations Review	68
3.4.2.6	Pre-Flight Readiness Review	68
3.4.2.7	Launch Readiness Review	69
3.5	Reliability, Maintainability, and Availability	71
3.5.1	Reliability, Maintainability, and Availability Program Plan	71
3.5.1.1	Reliability, Maintainability, and Availability Program Planning	71
3.5.2	Supplier Reliability, Maintainability, and Availability Requirements	71
3.5.3	Failure Reporting, Analysis, and Corrective Action System	71
3.5.4	Failure Review Board	72
3.5.4.1	Unverified Failures	72
3.5.5	Reliability Modeling, Allocation, and Prediction	72
3.5.5.1	Reliability Prediction Methodology	73
3.5.6	Reliability Analyses	73
3.5.6.1	Failure Modes, Effects, and Criticality Analysis	73
3.5.6.2	Fault Tree Analysis	74
3.5.6.3	Finite Element Analysis	74
3.5.6.4	Sneak Circuit Analysis	75
3.5.6.5	Worst Case Analysis	75
3.5.6.6	Electrical, Mechanical, and Thermal Stress Analyses	75
3.5.6.6.1	Thermal Stress Analysis	75
3.5.6.6.2	Mechanical Stress Analysis	75
3.5.6.6.3	Electrical/Electronic Stress Analysis	75
3.5.7	Mission Critical Items	75
3.5.8	Effects of Functional Testing, Storage, Handling, Packaging, Transportation, and Maintenance	76
3.5.9	Controlled and Limited Life Items	76
3.5.10	Reliability Growth Test Program	77
3.5.11	Accelerated Life Testing	77
3.5.12	Highly Accelerated Life Test	77
3.5.13	Highly Accelerated Stress Screen	77
3.5.14	Process Failure Modes and Effects Analysis	78
3.5.15	Environmental Stress Screening	78
3.5.16	Reliability Qualification Test Program/Demonstration	79
3.5.17	Maintainability Modeling, Allocations, and Predictions	79
3.5.18	Maintainability Analysis	79
3.5.19	Maintainability Demonstration	80
3.5.20	Availability Modeling, Allocations, and Predictions	80
3.5.21	Availability Assessment	80

3.5.22	Reliability, Maintainability, and Availability of Government Furnished Equipment/ Information	81
3.5.23	Reliability Surveillance of Deployed and Fielded Systems	81
3.6	Parts, Materials, and Processes Control Program	83
3.6.1	Parts, Materials, and Processes Plan	83
3.7	Integrated Test and Evaluation Program	85
3.7.1	Integrated Test and Evaluation Program Plan	85
3.7.2	Engineering Evaluation Tests	86
3.7.2.1	Integration Tests	86
3.7.2.2	Interoperability Tests	86
3.7.2.3	Test-Like-You-Fly	86
3.7.3	Qualification and Requalification Test Program	86
3.7.3.1	Qualification Program Plan	87
3.7.3.2	Qualification Tests	87
3.7.3.2.1	Qualification by Similarity	88
3.7.4	Acceptance Tests	88
3.7.5	Production Assessment Tests	88
3.7.6	Surveillance and Service Life Evaluation Tests	89
3.7.6.1	Surveillance and Service Life Evaluation Test Program Plan	89
3.7.7	Ground and Flight Tests	90
3.7.7.1	Test Risk Management Program	90
3.7.7.2	Critical Test Gate Process	90
3.7.7.3	Post Test Performance Analysis	91
3.7.7.4	Failure Review Process	91
3.7.8	Modeling and Simulation	91
3.7.9	Test Plans	91
3.7.10	Test Procedures	92
3.7.11	Test Reports	92
3.8	Test, Measuring, and Diagnostic Equipment and Standards	95
3.8.1	Selection and Design	95
3.8.1.1	Test, Measuring, and Diagnostic Equipment Configuration Documentation	95
3.8.1.2	Evaluation of Test, Measuring, and Diagnostic Equipment	95
3.8.1.3	Proofing, Qualification, and Correlation	96
3.8.2	Calibration and Maintenance	96
3.8.2.1	Calibration and Maintenance Procedures	96
3.8.2.2	Records and Analysis	97
3.8.2.3	Out-of-Tolerance Conditions	97
3.8.2.4	Calibration Standards and Reference Materials	97
3.8.3	General Test, Measuring, and Diagnostic Equipment and Standards Requirements	97
3.8.3.1	Intervals and Recall	97
3.8.3.2	Labeling	98
3.8.3.3	Sealing for Integrity	98
3.8.3.4	Removal of Test, Measuring, and Diagnostic Equipment and Standards	98
3.8.3.5	Test Station Logs	98
3.9	Interface Management	99
3.9.1	Interface Control Plan	99
3.9.1.1	Interface Control Plan Development	99
3.9.2	Interface Documentation	100
3.9.3	Interface Control Working Groups	100
3.9.4	Interface Change Notice	100
3.10	Configuration Management	103

3.10.1	Configuration Management Plan.....	103
3.10.2	Supplier Configuration Management	104
3.10.3	Configuration Identification.....	104
3.10.3.1	Product Information	104
3.10.3.2	Product Structure and Configuration Item Selection	104
3.10.3.3	Product Identifiers	104
3.10.3.3.1	Unique Software Identifiers	105
3.10.3.3.2	Identifying Individual Units of Product	105
3.10.3.3.3	Identifying Groups of Units of a Product	105
3.10.3.3.4	Department Of Defense Item Unique Identification	106
3.10.3.4	Document Identification	106
3.10.3.5	Configuration Baselines.....	106
3.10.3.5.1	Establishing Configuration Baselines.....	106
3.10.3.5.2	Types of Configuration Baselines	106
3.10.3.6	Interface Control	107
3.10.4	Configuration Change Management	107
3.10.4.1	Classifying Changes	107
3.10.4.1.1	Class I Engineering Change	107
3.10.4.1.2	Class II Engineering Change	108
3.10.4.2	Documenting Requests for Engineering Changes	108
3.10.4.3	Configuration Control Board	109
3.10.4.4	Change Effectivity Determination	110
3.10.4.5	Change Implementation and Verification.....	110
3.10.4.6	Change Management Process Applied to Variances	111
3.10.4.6.1	Requests for Waiver.....	111
3.10.4.6.2	Requests for Deviation.....	111
3.10.4.6.2.1	Restrictions on Waivers and Deviations.....	112
3.10.4.6.2.2	Classification of Waivers and Deviations	112
3.10.4.6.3	Review and Approval of Waivers and Deviations	112
3.10.5	Configuration Status Accounting.....	113
3.10.6	Configuration Audit.....	114
3.10.7	Configuration Management of Digital Data	114
3.10.7.1	Digital Data Identification	114
3.10.7.2	Data Status Level Management	114
3.10.7.3	Digital Data Transmittal	115
3.10.7.4	Data Access Control	115
3.11	Control of Nonconforming Items and Materials.....	117
3.11.1	Preliminary Review	117
3.11.2	Material Review Board	118
3.11.2.1	Material Review Board Membership.....	118
3.11.2.2	Material Review Board Dispositions	118
3.12	Fabrication and Quality	119
3.12.1	Manufacturing, Process, and Quality Control Planning	119
3.12.2	Process Selection and Development	119
3.12.2.1	Process Selection and Development Planning.....	119
3.12.2.2	Mission Critical Process Selection.....	120
3.12.2.3	Special Processes	120
3.12.3	Product Test and Inspection Plan	120
3.12.4	Fabrication and Quality Procedures.....	121
3.12.4.1	Fabrication and Process Procedures	121
3.12.4.2	Test and Inspection Procedures	121
3.12.4.3	Workmanship Standards	122
3.12.4.3.1	Connector Mating and Demating	122
3.12.4.3.2	Threaded Fasteners and Torque	122

3.12.5	Product Control during Fabrication	123
3.12.5.1	Product Identification and Handling	123
3.12.5.2	Product Protection	123
3.12.5.2.1	Electrostatic Discharge Controls	123
3.12.5.2.2	Contamination Control Program	124
3.12.5.2.2.1	Clean Rooms	124
3.12.5.2.3	Foreign Object Elimination Program	124
3.12.5.3	Product Status Indication	124
3.12.6	Fabrication Process Control	125
3.12.6.1	Process Qualification and Requalification Program	125
3.12.6.2	Fabrication and Quality Metrics	125
3.12.6.3	Fabrication Defects	126
3.12.6.4	Continuous Process Improvement	126
3.12.7	Fabrication Environmental Stress Screening	126
3.12.8	Fabrication Quality Verification	126
3.12.8.1	In-Process and Acceptance Test and Inspection	126
3.12.8.2	First Article Test and Inspection	127
3.12.8.3	Nondestructive Test and Inspection	127
3.12.8.4	Nonconforming Items Control	127
3.12.9	Fabrication and Quality Records	127
3.12.9.1	Fabrication Records	127
3.12.9.2	Quality Control Records	127
3.12.9.2.1	Closeout Photographs	128
3.12.10	Packaging, Handling, Storage, and Transportation of Product	128
3.12.10.1	Packaging	128
3.12.10.2	Handling and Storage	128
3.12.10.3	Preparation for Shipment and Transportation	129
3.12.11	Lifting Devices and Equipment Program	129
3.12.11.1	Identification of Critical Lifts	129
3.12.11.2	Lifting Devices and Equipment Program Certification	129
3.12.11.3	Identification of Critical Moves	130
3.13	Supplier Management	131
3.13.1	Supplier Selection	131
3.13.1.1	Safety and Mission Critical Supplier List	132
3.13.1.2	Conditional Source Approval	132
3.13.2	Supplier Ratings	132
3.13.3	Supplier Evaluations	133
3.13.4	Supplier Program Requirements	133
3.13.4.1	Supplier Management System	133
3.13.5	Procurement Process	134
3.13.5.1	Technical Requirements	134
3.13.5.2	Detailed Provisions	134
3.13.5.3	Procurement Document Review	135
3.13.5.4	Procurement Document Change Control	136
3.13.6	Control of Customer/Government Furnished Material	136
3.13.7	Government Source Inspection	136
3.13.8	Contractor Source Inspection	136
3.13.9	Receiving Inspection and Test	137
3.13.10	Intra-Corporate Work Transfers	138
3.14	Safety	139
3.14.1	Safety Program Requirements	139
3.14.1.1	Safety Policies	139
3.14.1.2	Safety Task Documentation	140
3.14.1.2.1	System Safety Program Plan	140

3.14.1.2.2	System Safety Hazard Analysis and Report	142
3.14.1.2.3	Safety Assessment Report.....	143
3.14.1.2.4	Safety Variance (Waiver/Deviation) Reporting	144
3.14.1.2.5	Engineering Change Proposal System Safety Reports	144
3.14.1.2.6	Integrated System Safety Program Plan.....	144
3.14.1.2.7	Health Hazard Assessment Report.....	145
3.14.1.2.8	Safety Incident/Near Miss Report	145
3.14.1.2.9	Management Trends Reports	145
3.14.1.2.10	Message Modification Technologies Reporting and Approval.....	146
3.14.1.3	System Safety Working Groups.....	146
3.14.1.4	Hazard Tracking.....	146
3.14.1.5	Safety Verification	146
3.14.1.6	Safety Defect/Deficiency Assessment.....	147
3.14.1.7	System Safety Program Reviews/Audits	147
3.14.2	System Safety Requirements.....	147
3.14.3	System Safety Engineering Approach	148
3.14.3.1	System Safety Hazard Identification and Analysis Methodology	149
3.14.3.2	Assessment of Mishap Risk.....	149
3.14.3.3	Risk Acceptance Authority.....	149
3.14.3.4	Mishap Investigations	149
3.14.4	Safety Design Criteria	150
3.14.4.1	Unacceptable Conditions.....	150
3.14.4.2	Design Constraints	150
3.14.4.3	Interlock Status and Restoration.....	151
3.14.4.4	Ignition System Safety Requirements	151
3.14.4.5	Fuze System Safety Requirements	151
3.14.4.6	Hazardous Materials Transportation.....	151
3.14.4.6.1	Lithium Batteries	151
3.14.4.7	Insensitive Munitions Design and Safety Tests	151
3.14.4.8	Ordnance Systems	152
3.14.4.9	Missile and Space Vehicle Pressure Systems	152
3.14.4.10	Orbital Debris	152
3.14.5	Safety and Health.....	152
3.14.5.1	Occupational Safety and Health	152
3.14.5.1.1	Hazardous Materials Management	152
3.14.5.1.2	Human Engineering	153
3.14.5.1.3	Lasers.....	153
3.14.5.1.4	Human Exposure to Radio Frequency.....	153
3.14.6	Test and Range Safety	153
3.14.6.1	Test Safety.....	153
3.14.6.2	Range Safety	154
3.14.6.2.1	Flight Termination System and Range Safety Tracking System Standards.....	155
3.14.6.2.2	Three-Tone Receivers	155
3.14.6.2.3	FTS Receiver Implementation Exclusivity.....	155
3.14.6.2.4	Flight Safety Analysis.....	155
3.14.7	Safety Critical Computing System Functions.....	155
3.14.8	Safety Critical Variables and Information Exchange Requirements	156
3.14.9	Software Safety	156
3.14.9.1	Software Coding Standard and Requirements.....	157
3.14.10	Software Maintenance Requirements for Safety Critical Computing Systems.....	157
3.14.11	Design and Development of Computer Systems.....	157
3.14.11.1	General Design Requirements	158
3.14.11.2	Design Verification and Validation	158
3.14.11.3	System Design Requirements for Computer Systems	158
3.14.11.3.1	Designed Safe States	158
3.14.11.3.2	Safe State Return.....	158

3.14.11.3.3	Safety Critical Data Isolation	158
3.14.11.3.4	Safety Critical Software Isolation	158
3.14.11.3.5	Input/Output Registers and Ports.....	159
3.14.11.3.6	Fault Detection	159
3.14.11.3.7	Circumvent Unsafe Conditions.....	159
3.14.11.3.8	Fallback and Recovery.....	159
3.14.11.3.9	Simulators	159
3.14.11.3.10	System Errors Log	159
3.14.11.3.11	Positive Feedback Mechanisms	159
3.14.11.3.12	Corruption of Computing Environment.....	159
3.14.11.4	Power-Up System Initialization Requirements	159
3.14.11.5	System Level Check	159
3.14.11.6	Operational Checks	160
3.14.11.7	Feedback Loops	160
3.14.11.8	Interface Control	160
3.14.11.9	BMDS Interface Control.....	160
3.14.11.10	Inter-CPU Communications	160
3.14.11.11	Data Transfer Messages	160
3.14.11.12	External Functions	160
3.14.11.13	Value Verification	160
3.14.11.14	Full Scale Representations	161
3.14.11.15	Safety Kernel	161
3.14.11.16	Inadvertent Jumps	161
3.14.11.17	Overwritten Safety Critical Functions.....	161
3.14.11.18	Safety Critical Computing System Functions User Interfaces.....	161
3.14.11.18.1	Processing Cancellation.....	161
3.14.11.18.2	Hazardous Function Initiation	161
3.14.11.18.3	Safety Critical Displays	161
3.14.11.18.4	System Response to Operator Actions.....	161
3.14.11.18.5	Safety Alerts.....	162
3.14.12	MDA Safety Integration	162
3.14.12.1	Integration Responsibility.....	162
3.14.12.2	Flow Down of Requirements from Contractor to Supplier	162
4.0	NOTES	163
4.1	Custodian.....	163
APPENDIX (A.1) Mission Assurance Implementation Plan Development and Approval		A-1
APPENDIX (A.2) Requirements Applicability Matrix		A-7
APPENDIX (B) MDA Core Metrics.....		B-1
APPENDIX (C) Workmanship Requirements.....		C-1
APPENDIX (D) Acronyms		D-1
APPENDIX (E) Definitions		E-1

Figures

Figure 3.14.3-1 System Safety Engineering Approach.....	148
---	-----

Tables

Table 2-1: Applicable Requirements Documents	3
Table 2-2: Applicable Guidance Documents.....	7
Table 3.14.3.3-1 Safety Risk Acceptance Authority	149

1.0 SCOPE

The MDA Assurance Provisions (MAP) encompass development, engineering, testing, production, procurement, and implementation of missile defense elements under the cognizance of MDA. The MAP provides a measurable, standardized set of Quality, Safety, and Mission Assurance requirements that Government and contractors apply to safety and mission critical items in support of evolutionary acquisition and deployment of MDA systems.

1.1 Purpose

The MAP establishes Quality, Safety, and Mission Assurance processes and actions through disciplined application of general system engineering; interface, configuration, and risk management; and quality, safety, and management principles needed to achieve mission success throughout the evolutionary acquisition process.

The implementation of MAP disciplines promotes continual process improvement and cost reductions by improving productivity, mitigating risk, and enhancing Quality, Safety, and Mission Assurance.

1.2 Applicability and Accountability

The MAP applies to Government and contractor organizations involved in planning, designing, developing, fabricating, testing, integrating, deploying, and supporting systems under the cognizance of MDA. The activity responsible for performing each requirement will be stated (i.e., Government, Contractor, or both). 'Government' will be used to include MDA/CR, MDA/DE, MDA/DT, MDA/DV, MDA/GD, MDA/QS, Program Offices, and other Government agencies. 'Contractor' will be used to imply prime contractors, subcontractors, subtier suppliers; assembly, integration, and operation facilities used in support of MDA ground and flight testing; and National laboratories.

Government and contractors involved in planning, designing, developing, fabricating, testing, deploying, and supporting MDA products and services shall establish and maintain accountability for fulfilling Quality, Safety, and Mission Assurance requirements herein. Accountability shall be documented through assignment of specific roles, responsibilities, and authorities.

1.2.1 Mission Assurance Implementation Plan

A Mission Assurance Implementation Plan (MAIP) will be established and maintained by MDA/DE, MDA/DT, and MDA/DV to describe how the MAP is implemented in their organization. Contents and tailoring requirements for a MAIP shall be IAW [Appendix A.1](#).

1.2.2 MAP on Contract

The MDA Program Office responsible for planning, design, development, fabrication, test, deployment, and support of MDA safety and mission critical products and services by contractors shall invoke the MAP on contract with an MDA Quality, Safety, and Mission Assurance Directorate (MDA/QS) and the cognizant MDA Program Office approved Requirements Applicability Matrix (RAM) ([Appendix A.2](#)). Tailoring of MAP requirements shall consider program objectives, maturity, and applicable acquisition life cycle phase(s). The Government and contractor shall comply with International Traffic in Arms Regulations (ITAR) restrictions for the MAP on contract and RAM tailoring when foreign contractors and foreign suppliers are used.

1.3 International Traffic in Arms Regulations

The Directorate of Defense Trade Controls (DDTC), in accordance with 22 U.S.C. 2778-2780 of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130), is charged with controlling the export and temporary import of defense articles and defense services covered by the United States Munitions List (USML).

The ITAR regulations dictate that information and material pertaining to defense and military related technologies (for items listed on the USML) may only be shared with U.S. Persons unless authorization from the Department of State is received or a special exemption is used.

1.4 Order of Precedence

In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence, unless otherwise noted or specified in the contract (work order/task order). Nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained. Conflicts between the MAP and other requirements documents shall be resolved by MDA/QS, MDA Office of Primary Responsibility (e.g., DE, DT), and the cognizant MDA Program Office.

Federal Acquisition Regulation (FAR) requirements are cited within the individual provisions of this document to provide definition, clarification, and guidance on requirements. The MAP does not alter the FAR requirements or inadvertently or intentionally impose additional criteria (requirements). Potential conflicts between MAP and FAR requirements shall be referred to the Contract Administration Office and MDA/DA for clarification and resolution.

2.0 APPLICABLE DOCUMENTS

The documents listed in Table 2-1: Applicable Requirements Documents are cited within the MAP text and form a part of this document to the extent specified herein. All documents cited within the reference shall be used as cited in the reference (i.e., requirement or guidance). For dated documents, only the cited revision applies. Table 2-2 identifies Applicable Guidance Documents. For undated documents, the latest revision of the reference document (including amendments), applicable at the time of contract award, applies unless a specific exemption has been obtained. Where MAP requirement text does not indicate specific document revision the revision annotated in this list is applicable. Requests for use of revisions to those documents not identified as BMDS Technical Core Standards shall be submitted to MDA/QS; for documents identified as BMDS Technical Core Standards, requests for variations or alternates shall be processed in accordance with MDA Directive 4122.01, BMDS Technical Core Standards. Table 2-1: Applicable Requirements Documents identifies BMDS Technical Core Standards cited within the MAP with an "X" in the BMDS Technical Core Standard column.

Table 2-1: Applicable Requirements Documents

Document Number	Document Title	Issue Date	BMDS Technical Core Standard
Aerospace Report No. TR-99 (1413)-1	Natural and Triggered Lightning Launch Commit Criteria	Jan 99	
AFSPC Manual 91-710	Range Safety User Requirements Manual (Volumes 1 through 7)	Jul 04	
AIAA S-080	Standard for Space Systems - Metallic Pressure Vessels, Pressurized Structures, and Pressure Components	1999	X
AIAA S-081	Standard for Space Systems - Composite Over Wrapped Pressure Vessels	2001	X
ANSI/NCSL Z540.3-2006	Requirements for the Calibration of Measuring and Test Equipment	2006	
ANSI Z136.1	Safe Use of Lasers	Jan 00	X
ANSI Z136.6	Safe Use of Lasers Outdoors	May 00	X
ANSI/ESD-S20.20-2007	ESD Association Standard for the Development of an Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)	2007	
ASME Y14.24	Types and Applications of Engineering Drawings	2009	
	Ballistic Missile Defense System Test Concept of Operations	Apr 09	
BMDS SEP Revision 2	Ballistic Missile Defense System (BMDS) Systems Engineering Plan (SEP)	Dec 13	
CMMI-DEV Version 1.3	Capability Maturity Model Integration (CMMI) for Development	Nov 10	
DOD 4145.26-M	DOD Contractor's Safety Manual for Ammunition and Explosives	Mar 08	

Document Number	Document Title	Issue Date	BMDS Technical Core Standard
DTR 4500.9-R	Defense Transportation Regulation		
FAR 46.4	Government Contract Quality Assurance		
FAR 52.245-1	Government Property	Jun 07	
FAR 52.246-2 through 52 246-8	Inspection Requirements		
IEEE C95.1	Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz	2005	X
IEEE 730	IEEE Standard for Software Quality Assurance Plans	Sep 02	
IEEE 730.1	IEEE Guide for Software Quality Assurance Planning	Dec 95	
IEEE 1012	Standard for Software Verification and Validation	Dec 04	
IEEE/ISO/IEC 14764	Standard for Software Engineering - Software Life Cycle Processes - Maintenance	2006	
IPC J-STD-001E (Class 3)	Requirements for Soldered Electrical and Electronic Assemblies	Apr 10	
IPC J-STD-001ES	Space Applications Electronic Hardware Addendum to Requirements for Soldered Electrical and Electronic Assemblies	Dec 10	
IPC/WHMA-A-620B (Class 3)	Requirements and Acceptance for Cable and Wire Harness Assemblies	Oct 12	
IPC/WHMA-A-620B (Class 3) Amendment 1	Requirements and Acceptance for Cable and Wire Harness Assemblies	Aug 13	
IPC/WHMA-A-620B-S	Space Applications Electronic Hardware Addendum to IPC/WHMA-A-620B	Jun 13	
IPC-2220 Series (Class 3)	Family of Design Documents		
IPC-6010 Series (Class 3)	Family of Board Performance Documents		
IPC-6012C (Class 3/A)	Qualification and Performance Specification for Rigid Printed Boards; Space and Military Avionics Deviations	Apr 10	
ISO/IEC 17025:2005	General Requirements for the Competence of Testing and Calibration Laboratories	May 05	
MDA Directive 3100.01	International Test Policy	Mar 10	
MDA Directive 3200.03	Test Review Policy	Mar 07	
MDA Directive 4122.01	BMDS Technical Core Standards	Jun 11	

Document Number	Document Title	Issue Date	BMDS Technical Core Standard
MDA Directive 4161.02	Item Unique Identification	Apr 10	
MDA Directive 5000.15	Ballistic Missile Defense System Requirements Traceability Process	Mar 13	
MDA Directive 6055.05	Failure Investigations	Apr 09	
MDA Directive 8315.01	Modeling and Simulation (M&S), Verification, Validation, and Accreditation (VV&A)	Jan 09	
MDA Directive 8315.02	Modeling and Simulation Program	Jan 09	
MDA Instruction 3000.07-INS	Ballistic Missile Defense System Ground Test Concept of Operations	Dec 12	
MDA Instruction 3058.01-INS	Risk Management	Apr 11	
MDA Instruction 5010.24-INS	Performing an Engineering Manufacturing Readiness Level Assessment	Jul 10	
MDA Instruction 6055.02-INS	Accident and Mishap Safety Investigations and Reporting	May 13	
MDA DX Memorandum	Updated Safety Risk Acceptance Authority	May 07	
MDA Manual 3000.05-M	Ballistic Missile Defense System Test Failure Initial Response	May 11	
MDA Manual 3500.01-M	Ballistic Missile Defense System Change Management Process	Oct 13	
MDA Manual 9420.03	Mission Execution Standards	Jan 11	
MDA Policy Memorandum No. 12	MDA Director's Safety Policy	Jul 09	
MDA Policy Memorandum No. 72	Safe Use of Message Modification Technologies	Jul 13	
MDA Test Risk Management Plan	Test Risk Management Plan	Apr 10	
MDA-QS-IPP-001	Mission Assurance Isolation Protection Profile (IPP), v1.0	Oct 12	
MDA-QS-003-PMAP-REV B	Missile Defense Agency Parts, Materials, and Processes Mission Assurance Plan (PMAP)	Mar 12	
MIL-STD-130N	Department of Defense Standard Practice Identification Marking of U.S. Military Property	Dec 07	
MIL-STD-464C	Electromagnetic Environmental Effects Requirements for Systems	Dec 10	
MIL-STD-810G	Environmental Engineering Considerations and Laboratory Tests	Oct 08	X
MIL-STD-882E	System Safety	May 12	

Document Number	Document Title	Issue Date	BMDS Technical Core Standard
MIL-STD-1316E(1)	Fuze Design, Safety Criteria for	Jan 99	X
MIL-STD-1472F(1)	Human Engineering	Dec 03	X
MIL-STD-1522A Notices 1, 2, and 3	General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems	Sep 92	X
MIL-STD-1576	Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems	Sep 92	X
MIL-STD-1686C	Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)	Oct 95	
MIL-STD-1901A	Munitions Rocket and Missile Motor Ignition System Design, Safety Criteria for	Jun 02	X
MIL-STD-2105D, Section 5.2	Hazard Assessment Test for Non-Nuclear Munitions	Apr 11	
MIL-STD-3022 W/Change 1	Documentation of Verification, Validation, and Accreditation (VV&A) for Models and Simulations	Apr 12	
NASA-STD-8719.9 W/Change 1	Standard for Lifting Devices and Equipment	May 02	
NASA-STD-8739.5 W/Change 2	Fiber Optics Terminations, Cable Assemblies, and Installation	Mar 11	
NAVSEAINST 9310.1B	Naval Lithium Battery Safety Program	Aug 04	
OSHA Form 174	Material Safety Data Sheet (MSDS)	Sept 85	
PDUSD(AT&L) Memorandum	Document Streamlining – Life Cycle Sustainment Plan	Sep 11	
Public Law 10 USC 141 Section 2389	Armed Forces Miscellaneous Procurement Provisions: Ensuring Safety Regarding Insensitive Munitions	Current Version	
Public Law 22 CFR Parts 120-130	International Traffic in Arms Regulations (ITAR)	Current Version	
Public Law 22 USC 2778-2780	Arms Export Control Act (AECA)	Current Version	
Public Law 91-596, 29 USC 651-678	Occupational Health and Safety Act	Current Version	
RCC-106	Telemetry Standards		
RCC-319	Flight Termination Systems Commonality Standard		
RCC-321	Common Risk Criteria for National Test Ranges		

Document Number	Document Title	Issue Date	BMDS Technical Core Standard
RCC-324	Global Positioning and Inertial Measurements Range Safety Tracking Systems Commonality Standard		
SAE AS9100C	Quality Management Systems – Requirements for Aviation, Space and Defense Organizations	Jan 09	
SMC-S-016	Test Requirements for Launch, Upper-Stage, and Space Vehicles	Jun 08	
S9310-AQ-SAF-010	Technical Manual For Batteries, Navy Lithium Safety Program Responsibilities and Procedures	Aug 04	
TB-700-2/ NAVSEAINST 8020.8/ DLAR 8220.1	Explosives Hazard Classification Procedures	Jan 98	X
49 CFR Parts 100-199	Transportation	Current Version	X

Table 2-2: Applicable Guidance Documents

Document Number	Document Title	Issue Date
	Risk Management Guide for DOD Acquisition Sixth Edition	Aug 06
DOD Directive 8320.03	Unique Identification (UID) Standards for a Net-Centric Department of Defense	Mar 07
DODI 8320.04	Item Unique Identification (IUID) Standards for Tangible Personal Property	Jun 08
IEEE 1633	Recommended Practices on Software Reliability	2008
IEEE/ISO/IEC 12207	Standard for Systems and Software Engineering – Software Life Cycle Processes	2008
M-2699-1.0	Ballistic Missile Defense System (BMDs) Technical Core Standards Management Handbook	Feb 14
MIL-HDBK-61A (SE)	Configuration Management Guidance	Feb 01
MIL-HDBK-189C	Reliability Growth Management	Jun 11
MIL-HDBK-344A Notice 2	Environmental Stress Screening (ESS) of Electronic Equipment	May 12
MIL-HDBK-470A Notice 2	Designing and Developing Maintainable Products and Systems, Volume I	May 12
MIL-HDBK-2155	Failure Reporting, Analysis and Corrective Action Taken	Dec 95
MIL-HDBK-2164A	Environmental Stress Screening Process for Electronic Equipment	Jun 96
MIL-HDBK-2165	Testability Handbook for Systems and Equipment	Jul 95

Document Number	Document Title	Issue Date
NASA-STD-5020	Requirements for Threaded Fastening Systems in Spaceflight Hardware as Guidance for Threaded Fastening Systems	Mar 12
NASA-STD-8739.4 W/Change 6	Crimping, Interconnecting Cables, Harnesses, and Wiring	Mar 11
NAS 412	Foreign Object Damage / Foreign Object Debris (FOD) Prevention	1997
NSS 1740.14	Guidelines and Assessment Procedures for Limiting Orbital Debris	Aug 95
S-2816-1.0	Ballistic Missile Defense System Requirements Traceability Handbook	May 13
SMC-S-001	Systems Engineering Requirements and Products	Jul 10

3.0 QUALITY, SAFETY, AND MISSION ASSURANCE PROVISIONS

3.1 Management

The Government and contractor shall establish and maintain fundamental management disciplines to plan, establish, and monitor a Quality, Safety, and Mission Assurance (QSMA) Program. It shall include requirements for internal and external communication, sharing information, mitigating risk, and encouraging continual improvement. This is accomplished by establishing effective management programs, including policy, planning, training, documentation, and review processes to execute the QSMA Program. The Government and contractor shall have a Quality Management System (QMS) that is compliant with requirements of SAE AS9100, Quality Management System – Requirements for Aviation, Space and Defense Organizations. Assurance related activities not covered by SAE AS9100 requirements are identified in the following sections and supplement SAE AS9100 requirements.

The Government and contractor shall establish and maintain those policies, procedures, or command media necessary to fulfill Missile Defense Agency Assurance Provisions (MAP) requirements. Where practical, MAP requirements should be satisfied through application of the Government's and contractor's documented and approved standard processes and programs rather than creating a new, separate set of processes to meet the MAP requirement's intent.

The contractor implementing procedures shall be identified in a QSMA Implementation Matrix, which defines how MAP requirements imposed herein, are implemented. The QSMA Implementation Matrix shall specify applicable MAP requirements, cross-referenced to applicable implementation procedures, instructions, and specifications. The matrix shall clearly delineate organizational accountability for implementation of MAP requirements. The matrix shall be stored in Integrated Digital Environment (IDE) [\(3.1.5\)](#).

3.1.1 Contract Reviews

The contractor shall establish and maintain a process for contract reviews to ensure that program and technical requirements are understood. Any requirement problems identified shall be resolved with the cognizant MDA Program Office. The review process shall be used to communicate requirements to various supporting organizations and disciplines within the program. Contractor program management shall conduct contract reviews with participation from affected disciplines (e.g., contracts, quality, manufacturing, engineering, configuration management, and supplier management). The contractor shall evaluate contract requirements using applicable criteria assuring:

- a. The capability to satisfy requirements is available.
- b. The requirements are consistent and cover customer needs.
- c. Adequate procedures are documented and implemented for handling changes to contract requirements and escalating problems.
- d. Procedures are documented and implemented for interface and cooperation among the parties, including ownership, warranty, copyright, licenses, and confidentiality.
- e. Acceptance criteria and procedures are documented and implemented in accordance with (IAW) requirements.

Amendments or modifications to contract requirements shall result in a review of requirement changes with affected disciplines by the contractor's program manager. Results of contract reviews shall be documented and stored in IDE [\(3.1.5\)](#).

3.1.2 Management Reviews

Management reviews discussed in SAE AS9100 shall also include information on results of metrics monitoring, internal audits, external audits, analysis of product data, and risk assessments. Output from management reviews shall include assessments related to effectiveness of systems used to implement QSMA requirements, including program and technical performance results. The Government and contractor shall use output of management reviews to continually improve effectiveness of the QSMA program. Contractor records from management reviews, including any actions assigned, shall be stored in IDE [\(3.1.5\)](#).

3.1.3 Technology Change Management

The contractor's top-level management shall define the organization's Technology Change Management policy for improving hardware, software, firmware, safety, quality, fabrication, productivity, and development time. This includes establishing responsibilities and authority for implementing policy, allocating resources for technology change management activities, and coordinating requirements and issues associated with technology change management at appropriate management levels within the organization. The contractor shall establish a program which identifies, selects, and evaluates new technologies; incorporates technologies that improve hardware, software, firmware, safety, quality, and fabrication; increases productivity; and decreases development cycle time.

3.1.4 Process Improvements and Core Metrics

The Government's and contractor's top-level management shall define and oversee the organization's program for implementing process development, assessment, and continual process improvement. The Government and contractor shall monitor, control, and report on the effectiveness of processes used during development, maintenance, and operations. The program shall address:

- a. Increasing quality and productivity.
- b. Decreasing development time and rework.
- c. Adopting new technologies and processes.
- d. Developing and improving processes and related process assets.
- e. Coordinating process development, assessment, and improvement across the organization.
- f. Ensuring safety [\(3.14\)](#).
- g. Processing noncompliances.

The contractor shall establish and maintain a measurement program to monitor and report on program and process effectiveness. The contractor shall develop an approach and methodology to identify and select metrics to monitor, control, and report on critical program and process requirements throughout the acquisition process. When analyzing and reporting metrics, the contractor shall assess the validity and performance of each metric. Metrics shall include parameters used for measuring continuous process improvement and for assessing effectiveness of QSMA requirements implementation throughout the supply chain. Metrics shall be made available to MDA/QS and the cognizant MDA Program Office, or designated representative(s).

3.1.4.1 MDA Core Metrics

The contractor shall establish and maintain a system for collection, monitoring, analysis, reporting and trending of MDA core metrics for hardware, software, and firmware work products and processes. The purpose of these core metrics is to provide top-level management with insight into critical areas and

processes (e.g., development, fabrication, and test) and to assist in identifying trends. Core metrics shall be reported to the cognizant MDA Program Office, MDA/QS, and MDA/DE.

Each MDA Program Office will negotiate a set of core metrics with the contractor, using Appendix B to address discipline in the processes and assess maturity of MDA products and services. At a minimum, the metrics will address the following five critical areas:

- a. Progress and Schedule – schedule, task completion, and progress as compared to baselined program plans.
- b. Growth and Stability - delivery of the required capability and management of volatility within defined management ranges.
- c. Funding and Resources - adequacy of funding and resources (including personnel) to perform software development work identified in baselined program plans.
- d. Adequacy, Quality, Safety, and Performance - evidence of the extent to which hardware, software, and firmware safely and securely meet program capability requirements, including key performance attributes, and that the delivered product safely and securely meets the user's intention without failure.
- e. Software Development Environment - the software productivity, languages selected, adoption of software development best practices, exhibited elements of reuse, and efficiency of the software development team.

The contractor shall establish a set of metrics that fully addresses the critical areas above in full consideration of life cycle phase, assessed risks, and program maturity. The contractor shall use metrics to help identify and mitigate risks, assess and improve development and fabrication processes, and ensure product quality. The contractor's metrics system shall include a process for adding, deleting, and modifying metrics as requested by the cognizant MDA Program Office.

3.1.5 Integrated Digital Environment

The contractor shall establish, operate, and maintain an Integrated Digital Environment (IDE) as the central repository for the contractor's program data and documentation as set forth below. The contractor shall maintain documents and data in electronic readable/searchable/parsable formats, such as text files. The contractor shall ensure that the IDE is configured with standardized digital tools and software to be used by contractor, safety and mission critical suppliers, and MDA. Documentation and data shall be available to external database management systems electronically and shall be extracted and processed without manual entry or file conversion. The location, directory structure, file naming conventions, and access shall be mutually agreed upon between the contractor and the cognizant MDA Program Office. Changes in data format, content, delivery frequency, or delivery method shall be approved by the cognizant MDA Program Office prior to incorporating changes. Selected MDA personnel shall have direct access via an on-line application to stored information at the lowest level necessary to expedite retrieval of essential documentation in support of program, pedigree, technical, and mission assurance reviews and other MDA activities requiring BMDS/MDA program documentation. The contractor shall provide systems that allow data to be readily transferred from the IDE to MDA systems and from MDA systems to the IDE. The contractor's configuration management tools shall be available, accessible, and configured to be usable by selected MDA personnel. The contractor shall use the IDE as the master library. The master library shall provide an index, by category for all program documentation that is sufficiently detailed to allow users direct access to a specific document. Documentation within the library shall be under documentation control with revision status, author, and file location clearly indicated. Previous revisions of documentation shall be available for retrieval.

In addition to items listed below (a through l), the contractor shall provide the following data through the IDE: engineering, test, configuration, safety, logistics, and maintenance and repair. Other related QSMA

data and documentation shall be available as negotiated by the cognizant MDA Program Office. The contractor shall provide:

- a. Networks to share and process unclassified and classified program data (e.g., calendar information, briefings and presentations, administrative information, working documents, plans, procedures, and program specifications).
- b. Change request processing system which includes, but not limited to: the need/reason for change, impact, priority, change category, description of change, products affected, list of drawings, documents, cost, schedule, hardware, firmware, and software (with release dates) that are affected by the change, and for change effectivity and Configuration Control Board (CCB) disposition.
- c. Product life cycle management tool that provides for storage, management, and control of technical and program data, including trades/analyses, drawings, documents, specifications, product support packages, and associated lists.
- d. Data Management (DM) tool used for scheduling, processing, tracking, and providing status of a contractor's/subcontractor's contract data delivery requirements.
- e. Tracking system database for hardware, firmware, software, and facility nonconformance trouble and failure records; Failure Review Board (FRB) decisions; Failure Reporting, Analysis, and Corrective Action System (FRACAS) Reports and Closure Statements; and Failure Investigation Reports and associated activities.
- f. Logistic database tool set to develop and manage Logistics Management Information, manage assets, track equipment ([3.1.14](#)), maintain inventory, process work orders, collect maintenance data, and track hardware and software configuration versions.
- g. Risk management database to identify risks, risk mitigation actions and results.
- h. Test Data Management tool to transfer data from the test sites to the Missile Defense Data Center and to support post-test reporting and data archiving (e.g., telemetry data, failure data, flight data, engineering data, and certification data).
- i. Linkage between other databases, so that data can be shared and searched across the IDE.
- j. Documentation control of documents stored on the IDE.
- k. Access to expert knowledge, success reports, and lessons learned from current and previous MDA programs.
- l. Documentation deliverables necessary to fulfill requirements cited throughout the MAP.

3.1.6 Risk Management Program

The Government and contractor shall establish and maintain a risk management program to continuously identify, analyze, mitigate, monitor, and report systems engineering process, product, technology, cost, schedule, and other program risks. Risk management process results shall be used for continual improvement and risk reduction. Program risks, whether primarily managed by the Government or by the contractor must be assessed and managed at the appropriate level. The Government and contractor shall establish and maintain risk management programs consistent with the Risk Management Guide for DOD Acquisition and shall report results of those programs in common format with consistent content IAW MDA Instruction 3058.01-INS. The Government and contractor shall report status of high and moderate risk areas and corresponding mitigation plans and activities at appropriate reviews (e.g., BMDS and Element reviews, and technical and mission assurance reviews). The contractor shall store risk management documentation and data in IDE ([3.1.5](#)). Additionally, when identified, any risk item

impacting a development, simulation, or test critical path, the contractor shall immediately notify the cognizant MDA Program Office. The cognizant MDA Program Office will then notify MDA/DE.

The contractor shall support MDA incremental risk assessments at their facilities and at mission critical suppliers in support of design and mission assurance reviews (3.4).

3.1.6.1 Risk Management Plan

The contractor shall develop a Risk Management Plan (RMP) that describes the risk management approach to be used on the program, including appropriate tools and techniques used to identify and mitigate risk. In the implementation of the plan, the following aspects shall be considered:

- a. Likelihood and severity of risks expected in demonstration of design performance, and with items having small design margins.
- b. Risks identified by reliability and safety analyses.
- c. Likelihood and severity of risks expected in development of new products, components, parts, materials, processes, and critical technologies.
- d. Likelihood and severity of risks expected in procurement, manufacturing, assembly, inspection, test, handling, storage, and transportation which may lead to unacceptable degradations in product quality.
- e. Likelihood and severity of risks anticipated in product utilization or service implementation.
- f. Risk identified by safety and mission critical suppliers.
- g. Risk of product quality degradation as the result of cost and schedule constraints imposed on the program.
- h. Effectiveness of risk reduction and control measures.
- i. Acceptability of residual risks.

The MDA risk management strategy includes a stakeholder collaborative effort in the overall risk management process. The RMP shall reflect this interaction. Qualitative and quantitative risk criteria shall be mutually agreeable between affected stakeholders. The plan shall include a process for flowing risks up through the required levels (e.g., from supplier through the cognizant MDA Program Office to MDA/DE). The contractor's plan shall be submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.1.7 Pedigree Program

The contractor and their suppliers shall have a formal pedigree program. The contractor shall develop pedigree data packages which support technical and mission assurance reviews, investigations and failure reviews, Independent Readiness Reviews, and critical events. Pedigree data shall be available from suppliers throughout the supply chain. Pedigree data shall be stored in IDE (3.1.5). The selection of items requiring pedigree data packages shall be based on criticality of the item to mission success of the system, single point failure potential, and first flight items. The pedigree data packages shall contain the complete chronological history from beginning of item build through final acceptance. The following information shall be included in the pedigree data package: design verification matrix (3.2.11); qualification data and reports; interface control data (3.9.2); complete inspection and test procedures with build inspection and test records, including physical and functional discrepancies, corrective actions, and repair and rework history; test history including failures and anomalies during item test, resolution, and retest; configuration status accounting information (3.10.5); manufacturing and process data; limited life

item data (3.5.9); closeout photographs (3.12.9.2.1); storage and transportation history; risk assessment and mitigation efforts associated with the product; and safety data (3.14.1.2).

3.1.8 Internal Evaluation Program

In addition to SAE AS9100 requirements, the Government and contractor shall evaluate their QSMA Program to determine compliance with QSMA requirements defined in the MAP and MDA Parts, Materials, and Processes Mission Assurance Plan (PMAP), as tailored by contract. Planning and periodicity for evaluations shall consider program phase, critical events and milestones, known problems, and level of activity in the functional area. Evaluations shall consist of reviews of QSMA disciplines and product conformance.

Internal evaluations of QSMA disciplines shall be performed to determine adequacy and implementation of policies and procedures used to satisfy QSMA requirements. Product conformance evaluations shall be performed to review fabrication, software media generation, test, and inspection operations. Evaluations shall assess effectiveness of processes used for assuring product conformance to applicable drawings, specifications, and procedures and shall include random assessment of product conformance to applicable drawings, specifications, and procedures.

Summaries of evaluations and corrective actions taken shall be prepared and distributed to internal top-level corporate management and stored in IDE (3.1.5).

3.1.9 Training and Certification Program

In addition to SAE AS9100 requirements, the Government and contractor shall establish, implement, and maintain a training and certification program to ensure sufficient program knowledge and personnel skills are developed and sustained. Government and contractor personnel shall have necessary skills and knowledge to perform their assigned activities.

The program shall include a method or procedure by which training needs are identified, provided, and assessed. Training for the organization and project processes shall be coordinated across the organization. The training program shall include:

- a. Review of project requirements to establish and make timely provision for developing resources and skills required by management and technical staff. Review results shall be documented in training plans. The types and levels of training and categories of personnel needing training shall be determined. A training plan addressing implementation schedules, resource requirements, and training needs shall be developed and documented. Training records shall be maintained.
- b. Development of training manuals, including presentation materials used in providing training.
- c. Training plans that identify the group or organization responsible for fulfilling training needs. Additionally, the Government and contractor shall develop training standards and procedures defining how software training courses are to be selected, developed, and maintained.
- d. Identification of the training subject, which includes specific tools, techniques, methodologies, and computer resources to be used for development, maintenance, and management of the product.

The Government's and contractor's management shall ensure the correct composition and categories of appropriately trained personnel are available for planned activities and tasks.

3.1.9.1 Training

The Government and contractor shall establish and maintain a training program for personnel whose work relates to, influences, or has an effect on quality or reliability of the product. Particular emphasis shall be given to new products, upgrades, and sensitive or hazardous manufacturing processes or materials. Personnel shall be proficient in their assigned tasks. Objective evidence of proficiency shall

be maintained IAW industry standards (3.12.4.3) and be available for review. Training needs shall be periodically assessed to determine requirements for additional training. The training program shall be evaluated on a periodic basis for consistency with, and relevance to, the organization's needs.

3.1.9.2 Certification

The Government and contractor shall establish and maintain a program for certification of personnel responsible for operation, test, inspection, or control of special processes (3.12.2.3) and equipment (3.12.11.2) that require certified skills. Criteria for determination of which processes require personnel certification shall be documented. The Government and contractor shall develop and maintain a list of skills and personnel requiring certification. Certification shall include a training program and a testing procedure to ensure proficiency. Documented evidence of individual certifications shall be readily available to, and used by, the immediate supervisor in assigning personnel for specific tasks. Results of tests on which the certification was granted shall be maintained. A period of certification effectivity shall be specified for each skill. Until properly recertified, personnel not exhibiting required proficiency shall be excluded from operations involved. The impact to any end items produced by personnel with expired certification shall be assessed. Test, inspection, and evaluation results shall be used as indicators for recertification regardless of the established period.

3.1.10 Problem and Failure Reporting and Corrective Action System

The Government and contractor shall establish and maintain a closed loop problem and failure reporting and corrective action system. The system shall include reporting of problems and failures, investigations, analyses, and performance of actions to correct problems and failures and preclude recurrence. Government and contractor procedures shall define the level and detail of documentation, dependent on the nature and criticality of the problem and failure. Problem and failure reporting shall include identification of items and conditions experienced. The Government and contractor shall investigate problems and failures to determine trends and need for analysis and corrective action. As a result of the investigation, the Government and contractor shall conduct problem and failure analysis to determine root cause of the problem or failure. All problems and failures identified and resulting corrective action shall be recorded and stored in IDE (3.1.5). Failure reporting and analysis impacting reliability, maintainability, and availability is described in 3.5.3.

The following actions shall be taken by the Government and contractor and documented:

- a. Corrective action shall be recommended and planned, an expected completion date established, and the organization identified that is responsible for performing corrective action.
- b. Corrective action shall be accomplished in a timely manner.
- c. Follow-up verification shall be performed to ensure completion and effectiveness of corrective action.

3.1.11 Data Exchange Programs Participation

The contractor and their suppliers shall participate in both Government Industry Data Exchange Program (GIDEP) and MDA Assurance Advisory Reporting System. New GIDEP alerts and MDA Assurance Advisories are received by each participant's coordinator, screened, and forwarded to the appropriate program or functional group for action. If a formal response is required by a MDA Assurance Advisory, instructions for action will be stated in the Advisory. Contractors and their suppliers shall generate new GIDEP alerts based on guidelines established by GIDEP. Contractors and their suppliers shall submit data and documentation appropriate for an MDA Advisory to MDA/QS for review, approval, and distribution. The contractor shall provide technical assistance to their suppliers who are not GIDEP and MDA Advisory participants.

3.1.12 MDA Insight and Oversight

Insight is a method used by MDA to gain an understanding of contractor's progress in meeting contractual requirements through observation, evaluation, and participation. The contractor shall provide MDA with open access to all matters and data relating to the contract. The access shall include, but not be limited to: facilities; meetings such as program reviews, technical interchange meetings, failure review boards, and change control boards; audits; program activities such as test events; training programs; information and analyses for any anomalies or issues occurring during fabrication, assembly, test, handling, or transportation which affect system integrity; and all data directly related to the program. The Government may offer feedback to the contractor for consideration. Insight shall be extended to MDA personnel and their designated representative(s).

Oversight of MDA programs shall be performed by MDA Assurance Representatives and MDA representatives. Oversight will include participation in QSMA activities, mandatory Government inspections, and MDA evaluations.

Personnel performing MDA insight and oversight shall protect contractor activities and information received or accessed from unauthorized disclosure.

3.1.12.1 MDA Assurance Representatives

Missile Defense Agency Assurance Representatives (MAR) will participate in or perform QSMA activities at contractor, subcontractor, supplier facilities, and National Laboratories. Activities may include but are not necessarily limited to engineering walkdowns, foreign object debris walkdowns, facility assessments, MDA evaluations, mission focus audits, manufacturing assessments, and technical and mission assurance reviews.

The contractor shall provide MARs with documents, records, equipment, and working areas within the contractor's facilities. The contractor shall make support services and office space available for resident MARs.

3.1.12.2 MDA Inspections

The MDA/QS and its delegated representative(s) maintain the right to perform inspections per Federal Acquisition Regulation 52.246 and quality assurance functions IAW Federal Acquisition Regulation 46.4. The Defense Contract Management Agency (DCMA) is used by MDA to perform Mandatory Government Inspections (MGIs) and quality assurance functions per letter of delegation.

Mandatory Government Inspections are formal inspections performed by DCMA and are hold points required prior to operations proceeding. The DCMA ensures MGIs are specifically identified in prime contractor's process plans and procedures, and flowed down to safety and mission critical suppliers. The DCMA shall ensure MGIs are placed at critical processing points for all safety and mission critical assemblies when:

- a. Critical, Major, and Minor Classification of Characteristics are specified on safety and mission critical item drawings or specifications.
- b. Noncompliance of safety or mission critical attributes can result in loss of life or loss of mission. Safety or mission critical attributes include hardware characteristics, manufacturing process requirements, operating conditions, and functional performance criteria.

The Government shall ensure MGIs are placed at critical processing points for safety and mission critical assemblies including any stage of manufacture or performance of services, or in any event before acceptance as may be necessary to determine that the supplies or services conform to contract requirements. As a minimum, the following specific areas are identified as MGI points; additional areas may be added where MDA deems a risk to product exists.

- a. End item mates, shroud mates and closeout operations at system, subsystem, and integration level.
- b. Safety and mission critical non-COTS electronics boxes prior to closure.
- c. Critical lifts.
- d. Critical software load onto flight vehicle.

The preceding areas above are not all inclusive. The DCMA, MDA/QS, and the cognizant MDA Program Office team will collaborate to identify additional areas for inspections. Proposed changes to MGIs shall be submitted to the cognizant MDA Program Office, MDA/QS and the responsible MDA/QS Mission Assurance Representative for review and approval.

3.1.12.3 MDA Evaluations

Management and work activities, operations, documentation, software, and metrics of the contractor and suppliers are subject to onsite evaluation, review, survey, facility assessment, and inspection by MDA/QS, cognizant MDA Program Offices, designated representative(s), and their designated independent assurance agency. The contractor shall grant access to MDA/QS, cognizant MDA Program Offices, and their designated representative(s) to conduct planned evaluations. Resources and an acceptable work area shall be provided to assist with the evaluation, while allowing minimal disruption to work activities. The contractor shall provide documents, records, and equipment required to perform QSMA activities. The contractor shall support MDA evaluations and provide timely corrective actions, as required.

3.1.13 Program Reviews

The contractor shall support periodic MDA or the cognizant MDA Program Office reviews to report program progress, risks, and status. Contractor's support shall include hosting, participating, preparing meeting minutes, and responding to review action items.

3.1.14 Government Furnished Material, Equipment, or Information

The contractor shall comply with SAE AS9100 and the following when the Government furnishes materials, equipment, or information:

- a. Perform examination upon receipt, consistent with practicability, to detect damage resulting from transit.
- b. Inspect to verify quantity, completeness, and proper identification.
- c. Handle and store the material or item in a manner to guard against damage, deterioration, and disclosure.
- d. Periodically inspect the stored material, item, or information to ensure adequate storage conditions and to guard against damage, deterioration, and disclosure during storage.
- e. Perform required maintenance and calibration.
- f. Establish controls for proper use or disposition.

The contractor shall report to the Government Contracting Officer any Government Furnished Material, Equipment, or Information that is lost, found damaged, malfunctioning, exposed to conditions which could lead to degradation, or that is otherwise unsuitable for use. In the event of damage or malfunction during or after installation, the contractor shall determine and record probable cause. Individual decisions regarding particular Government Furnished Material, Equipment, or Information shall be documented in the contract file.

3.1.14.1 Contractor Acquired Property

The contractor shall comply with FAR 52.245-1 Government Property requirements when property is acquired as a direct cost to the Government to fulfill contract requirements. Accountability, handling and storage, maintenance and calibration, and reporting of problems or damage shall be similar to Government Furnished Material and Equipment.

3.1.15 Repair, Refurbishment, and Modification

The contractor shall develop and document methods, procedures, and standards for performance of repair, refurbishment, and modification of returned Government owned products. Standards for acceptable and unacceptable conditions shall be prepared and shall define any allowances for mechanical wear during the acquisition process of the product. Standards and procedures shall be of sufficient detail for use by repair activities and submitted to the cognizant MDA Program Office or designated representative(s) for review and approval. Products shall be:

- a. Verified as to condition and configuration.
- b. Controlled to prevent commingling of serviceable and unserviceable items.
- c. Assessed to determine actions required for restoring the product to an acceptable condition.

The contractor shall establish processes to be applied when a reported failure cannot be confirmed upon receipt. The process shall define additional actions to be taken, including number and nature of tests necessary, retest criteria and approval, test facilities, and personnel required. Standards and procedures shall be of sufficient detail for use by repair activities and submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that the standards and procedures are submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

For contractor-owned product subject to repair, the requirements in 3.11 apply.

3.1.16 Responsible Engineer

The contractor shall assign Responsible Engineers (RE), who are accountable for Configuration Items (CI) (3.10.3.2). The REs shall be involved in all aspects of CIs including design and development, configuration management, manufacturing and test; supplier management, nonconformance documentation and review, associated risks and risk management, safety, operation readiness and certification, acceptance and delivery, and performance measurement.

The contractor shall ensure REs are properly trained (3.1.9) and qualified to governing regulations and compliance requirements associated with each CI. A qualified RE shall have the technical education and experience including the basic principles of design, manufacturing, and test associated with the CI. Contractors shall establish criteria for retraining.

The REs shall have the responsibility and technical authority for assuring the CIs are ready for use, and meet or exceed end item requirements.

3.2 Design and Development

The Government's and contractor's design and development program shall ensure required system capabilities are translated into a documented, integrated design solution; and verification is performed to ensure the solution meets requirements. The program shall ensure functional and performance requirements and internal and external interfaces are identified, classified, achieved, and controlled. The program shall use an integrated product and process development and iterative systems engineering approach to ensure all aspects of the product's life cycle are considered during the design and development process and desired outputs are achieved to ensure mission success. Verification and validation activities associated with system engineering processes shall be performed IAW documented plans and procedures. Verification and validation results shall be documented and retained. Drawings and specifications shall be generated to document the design solution and shall be controlled IAW [3.10](#). The design and development program shall be executed IAW policy supported by controlled engineering manuals, procedures, and guidelines that implement fundamental design principles, practices, and processes. The Government and contractor shall establish and maintain plans to manage and control design and development project activities. Requirements of this section apply to all new designs, redesigns, block changes, and modifications.

3.2.1 Integrated Product and Process Development

The contractor shall establish and maintain a process that integrates all design and development activities, through the use of multi-disciplinary teams, to concurrently balance the product design and its associated fabrication, manufacturing, and supportability processes to achieve life cycle system cost and performance objectives. The multi-disciplined Integrated Product Teams (IPT) shall represent all necessary specialties, functions, disciplines, and allow for participation of the cognizant MDA Program Offices, including MDA designated technical representative(s).

This process includes defining critical characteristics of the product, negotiating dependencies, and documenting acceptance criteria. Engineering functions within each IPT shall work together to:

- a. Monitor and coordinate technical activities and resolve technical issues to include safety risks ([3.14](#)).
- b. Identify, negotiate, and track critical dependencies.

The contractor shall develop and maintain a process to manage issues that cannot be resolved by group participants. In addition, the contractor's processes shall set forth rules for ensuring support tools used by different engineering groups are compatible.

3.2.2 Peer Reviews

The Government and contractor team shall conduct engineering peer reviews throughout planning, design, and development to identify and resolve technical issues and concerns before formal system level reviews ([3.4](#)). Engineering peer reviews for hardware, software, and firmware are required during all phases of the program life cycle as a key component of the Government's and contractor's quality, safety and mission assurance program. Peer reviews shall be conducted at the subsystem and lower levels by independent Subject Matter Experts having current detailed knowledge of the design specialties and processes associated with the item under review. The purpose of peer reviews is to substantiate a detailed understanding of the design's technical ability to meet all of its performance and interface requirements, to surface correctable problems early, identify risks, and to ensure best known practices are used to enhance design robustness by avoiding known or predictable problems.

3.2.3 Technical Performance Measurement

The contractor shall establish and maintain a process that provides a method of measuring Technical Performance Measurements (TPM). TPMs are derived from the system requirements to provide a cross section or representative sample of measures that define key system or product performance or high program risk. Each TPM shall be reviewed at least annually to determine their continued relevance and

effectiveness. Changes (additions/deletions) in TPMs shall be coordinated with MDA/DE and the cognizant MDA Program Office. Metrics shall be established to provide visibility into actual versus planned performance for TPMs. Contractor TPM trend data shall be evaluated and results shall be included in the risk management program (3.1.6).

3.2.4 Systems Engineering for Design

The Government's and contractor's system engineering process shall be used to translate mission and operational requirements and objectives, functional and performance requirements, design constraints, interface and interoperability requirements, statutory and regulatory requirements, and other applicable input requirements into an integrated design solution through concurrent consideration of all life cycle needs.

The Government will perform systems engineering using the Ballistic Missile Defense System (BMDS) Systems Engineering Plan (SEP). Throughout the MAP the Ballistic Missile Defense System Systems Engineering Plan will be abbreviated as the BMDS SEP. The contractor may use SMC-S-001, Systems Engineering Requirements and Products as a guide when performing systems engineering.

3.2.4.1 Element Systems Engineering Plan and Systems Engineering Management Plan

Each BMDS Element shall produce an Element Systems Engineering Plan (SEP) or Systems Engineering Management Plan (SEMP) that expands upon the BMDS SEP by describing the Element level planning details. Element level SEPs and SEMPs will be reviewed and approved by MDA/DE.

3.2.4.2 Contractor Systems Engineering Management Plan

The contractor shall develop a Systems Engineering Management Plan (SEMP) that describes design, engineering, technical management disciplines and processes, and technical responsibilities and authorities that support a system or product throughout its life cycle. The contractor's SEMP shall be submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office and MDA/DE. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

The SEMP shall address the following areas, as a minimum:

- a. Technical Program Planning and Control: Technical program tasks that must be planned and implemented in fulfillment of system engineering management objectives; organization responsibilities and authority for system engineering management including control of subcontracted engineering; levels of control established for performance and design requirements and control methods; plans and schedules for the design, development, assembly, integration, test and evaluation functions; and documentation control. The following areas are applicable to both hardware and software engineering activities:
 - 1) Technical program tasks planning.
 - 2) Engineering program integration.
 - 3) Contract work breakdown instruction and specification tree.
 - 4) Program reviews.
 - 5) Design reviews.
 - 6) Interface control.
 - 7) Risk Management.

- 8) Engineering testing.
- 9) Supplier requirements.
- b. System Engineering Processes: This section shall describe system engineering processes applied to define system design and test requirements; system engineering required to define system performance parameters and preferred system configuration; and planning and controls of technical program engineering disciplines. A narrative shall be included describing the contractor's proposed plans, processes, and procedures for the following elements of the system engineering process:
 - 1) Operational requirements.
 - 2) Feasibility analysis.
 - 3) Trade studies.
 - 4) System architecture.
 - 5) Technical performance measurement.
 - 6) Functional allocation.
 - 7) Requirements analysis and allocation.
 - 8) Synthesis, analysis, and design optimization.
 - 9) Technical interface compatibility.
 - 10) Configuration management.
 - 11) Design reviews.
 - 12) Producibility analysis.
 - 13) Maintenance concept.
 - 14) Training programs for users.
 - 15) Test and evaluation.
 - 16) Logistics support analysis.
- c. Engineering Specialty Integration: Methods by which the contractor proposes to integrate engineering efforts. It shall include a summary of each specialty program and cross reference the individual plans covering such specialty programs. Engineering specialty integration shall be discussed as well as the relationship of engineering with overall logistic efforts, including fault isolation methods (automatic, semiautomatic, and manual) and their documentation, and how support equipment is identified. Specialty areas in the overall engineering design and development include:
 - 1) Reliability and maintainability.
 - 2) Software.
 - 3) Quality.
 - 4) Parts, materials, and processes.

- 5) Human factors and safety.
- 6) Environmental, Safety, and Occupational Health.
- 7) Risk Management.
- 8) Configuration Management.
- 9) Data management.

3.2.5 Design for Interoperability

The Government and contractor shall establish and maintain a design engineering process that ensures interoperability with other MDA systems. The contractor shall coordinate with the cognizant MDA Program Office to establish, document, and control interface requirements necessary to ensure interoperability with other affected MDA systems. The cognizant MDA Program Office will coordinate interoperability requirements with MDA/DE and MDA/BC. Interoperability requirements identified during the systems engineering process shall be incorporated into the design's interface control documentation (3.9.2) and evolve consistent with the evolutionary acquisition approach. Interoperability requirements for a design shall be specified at a level of detail that allows for verification and test.

3.2.6 Design for Producibility

The Government and contractor shall establish and maintain a design engineering process that makes producibility of the design an early priority in the design and development effort. The contractor shall concurrently develop product designs and the required manufacturing processes to be used during fabrication and production. Manufacturing processes selected shall be statistically capable and have adequate capacity to meet expected production rate. The product shall be designed in such a manner that fabrication and manufacturing methods and processes have flexibility in producing the product at a reasonable cost while maintaining required functionality, performance, quality, and reliability. As part of the design for producibility, the contractor shall identify and document key characteristics as defined in SAE AS9100. Problem areas shall be identified early in the design process to ensure product designs, which:

- a. Minimize variability in the manufacturing process.
- b. Achieve higher quality within cost and schedule.
- c. Allow for insertion of new technologies to achieve increased producibility.
- d. Increase systems reliability.

3.2.7 Design for Testability

The Government and contractor shall ensure that design for testability is a priority. Basic testability or mission testability requirements shall be used to establish baseline requirements for designers. The contractor shall establish and maintain a testability program that defines the functional test parameters and the most efficient method and point at which the item will be tested. The testability program shall include:

- a. Establishment of sufficient, achievable, and affordable diagnostic concept and testability requirements for built-in (Built-In Test/Built-In Test Equipment (BIT/BITE)) and off-line test performance.
- b. Integration of testability into requirements and systems during the design process in coordination with the Integrated Test and Evaluation Program (3.7) and maintainability design process.

- c. Evaluation of the extent to which the design meets testability requirements.
- d. Inclusion of testability in the program review process.
- e. Testability Modeling, Allocations, and Predictions.

3.2.7.1 Testability Program Plan

The contractor shall develop, maintain, and submit a Testability Program Plan. The Testability Program Plan shall be submitted in IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. The Testability Program Plan may be an independent document or included within the contractor's SEMP or Reliability, Maintainability, and Availability Program Plan.

Testability Program Plan shall address:

- a. Work to be accomplished for each testability task.
- b. Time phasing of each task and its relationship to other tasks.
- c. Organizational element that has overall responsibility and authority for implementation of the testability program.
- d. Data interfaces between the organization responsible for testability and other related disciplines.
- e. Method by which testability requirements will be integrated with other design requirements and disseminated to design personnel and suppliers.
- f. Method by which integration and compatibility between testability and other diagnostic characteristics (e.g., technical information, personnel, and training) will be accomplished.
- g. Testability design guides and testability analysis procedures to be used.
- h. Procedures for scheduling, conducting, and documenting testability design reviews.
- i. Testability submissions and their review, verification, and utilization.
- j. Methods for demonstrating and validating diagnostic and testability requirements.
- k. Procedures for identifying testability related problems and corrective action.
- l. Procedures and controls to ensure contractor's testability practices are consistent with overall system or equipment requirements.

The contractor may use MIL-HDBK-2165 as additional guidance for testability tasks.

3.2.8 Design for Supportability

Supportability analyses shall be an integral part of the systems engineering process to ensure the product designed and developed meets the Government's planned logistics support approach. During the initial stages of the design and development process, the contractor shall coordinate with the cognizant MDA Program Office to identify and document a product support strategy as reflected in their Life Cycle Sustainment Plan (LCSP) as defined in PDUSD(AT&L) Memorandum, Document Streamlining – Life Cycle Sustainment Plan. The LCSP shall be submitted into IDE (3.1.5) and marked for approval by the

cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.2.9 Design for Commercial and Non-Developmental Items

The contractor shall establish and maintain a system to control design selection, evaluation, acceptance, and support of Commercial-Off-The-Shelf (COTS) and Non-Developmental Items (NDI), including hardware and software. If COTS/NDI products are used in MDA systems, subsystems, or assemblies, the contractor shall ensure COTS/NDI items meet all functional and interface requirements. The COTS/NDI shall be selected and qualified (MDA-QS-003-PMAP, Appendix C, paragraph 1.2 and 1.3) to operate in the intended application. The contractor shall verify COTS/NDI meet or exceed performance, quality, reliability, environmental, and survivability requirements, and develop a strategy for supporting or upgrading products throughout the system life cycle. The contractor shall also ensure that COTS Information Assurance products (e.g., routers, switches, servers, and communication equipment) planned for use in MDA hardware shall be limited only to those which have been evaluated and validated jointly by the cognizant MDA Program Office and the National Security Agency in accordance with the criteria defined in MDA-QS-003-PMAP paragraph 3.10.

3.2.9.1 COTS/NDI Design Strategies

When COTS/NDI are used the design strategies shall:

- a. Use form, fit, and function requirements to query the market.
- b. Begin market analysis early in program planning. Market analysis shall consider stability of the market for each item and projected technology advances, including quality, stability, and quantity of suppliers who provide products for each commercial and non-developmental item.
- c. Assess availability, relevance, and adequacy of design documentation, reliability data, performance data, and quality data; or, if needed, develop a mitigation plan to account for the lack of data.
- d. Design systems to accommodate insertion of new technology. When selecting COTS/NDI for inclusion in the design, the contractor shall include consideration of hardware, software, and firmware support as follows:
 - 1) Hardware: Refresh cycle, availability and capability of vendor supported repair or alternate repair support, warranty cost and coverage, Total Ownership Cost (TOC), vendor technical and design support, sole source or multi-vendor availability, remaining program life, and availability of technical data package purchase rights.
 - 2) Software and Firmware: Vendor technical and design support or alternate support, revision schedule, remaining program life, compatibility with other software and operating systems, application programming interface, cost of licenses and upgrades, TOC, stability of product, projected revisions, problem history, any known software issues or defects, and availability of technical data package purchase rights.
- e. Use open system architecture with strict adherence to commercial standard interfaces for hardware and software.
- f. Assure the strategy considers mission and environmental requirements and margin.
- g. Develop a procurement strategy for determining COTS/NDI viability for specific systems.
- h. Require extensive compatibility testing of the product at both subassembly and system levels.
- i. Test COTS/NDI spares functionally at the system or subsystem level using operational software.

- j. Produce vendor item control drawings, controlled IAW [3.10](#), documenting the engineering description and acceptance criteria for COTS/NDI. The vendor item control drawing shall provide a suggested source of supply, the vendor's item identification, and sufficient engineering definition for acceptance of interchangeable items within specified limits.
- k. Define a COTS spare policy for times when licenses and warranties expire before product spares are used.

3.2.10 Requirements Traceability and Verification Matrix

The Government shall perform requirements traceability in accordance with MDA Directive 5000.15, Ballistic Missile Defense System (BMDS) Requirements Traceability Process, which establishes policy and assigns responsibilities for BMDS requirements traceability from the system level through the subsystem allocated levels. The BMDS Requirements Traceability Handbook, S-2816-1.0, provides detailed process guidance for traceability activities, and establishes triggers and timelines for initiating and executing requirements traceability within the MDA Systems Engineering Process.

The contractor shall establish and maintain a system for providing traceability to hardware, software, and firmware and ensure specification and interface requirements are implemented in the design, including any COTS/NDI used, and verified. Each requirement contained in system specifications, subsystem specifications, equipment specifications, software/firmware requirements specifications, interface control documents, coordination drawings, and any other documents containing technical requirements shall be traceable to the demonstration, analysis, test, or inspection document in which requirements are verified. Bi-directional traceability shall be established from the source requirement down to its implementation level requirements and from implementation level requirements back to the source.

The contractor shall create and maintain a requirements traceability and verification matrix. For each requirement, the requirement traceability and verification matrix identifies the method of verification (analysis, inspection, demonstration, or test) and reference to verification results. The requirements traceability and verification matrix shall be controlled to ensure emerging requirements are documented and have performance verification methods assigned.

3.2.11 System Design Verification and Validation

The Government and contractor shall perform verification and validation.

The Government and contractor shall perform system design verification throughout the life cycle to assure that the design output meets the design input requirements. Design verification shall:

- a. Verify that each product defined by the system design solution conforms to a validated set of requirements of the selected physical solution representation.
- b. Verify that the set of defined system technical requirements agrees with the validated set of user needs and expectations.

All internal and external design interfaces shall be upward and downward traceable to their source requirement. The requirements traceability and verification matrix ([3.2.10](#)) shall be used to trace verification methods to a validated set of requirements.

The Government and contractor shall perform system design validation to demonstrate mission capabilities are met. Validation activities include, as appropriate: test, simulation, demonstration, or other applicable methods. The Government and contractor shall perform system design validation of product against its requirements baseline established during requirements analysis. System design validation shall consist of:

- a. Evaluation of product against its requirements baseline to ensure it represents identified MDA expectations and project, contractor, and external constraints.
- b. Technical assessment of product against its requirements baseline to determine whether the full spectrum of possible system operations and system life cycle support concepts has been adequately addressed.

Design verification and validation documentation shall consist of data, results, and reports from tests, inspections, demonstrations, calculations, analyses, and other relevant verification and validation activities. Design verification and validation testing activities shall be planned, controlled, reviewed, and documented to assure tests are performed IAW specifications and requirements pertaining to test plans (3.7.9) and test procedures (3.7.10).

3.2.12 Safety and Environmental Requirements

The Government and contractor shall ensure that the system design complies with safety and environmental statutes, regulations, policies, agreements, and provision 3.14. Selection and use of energetic materials and design of munitions and other explosive components, materials, or systems shall comply with Department of Defense (DOD) explosives safety requirements.

3.2.13 Open Systems Design and Standards

The Government and contractor shall implement an open systems design strategy in the development of MDA products that maximizes opportunities for reuse of existing technologies, previously designed product, and facilitates product upgrades. Open systems architectures and design standards shall ensure interoperability and compatibility in the system and product designs. Open system designs and standards shall be selected and controlled through the systems engineering process.

3.2.14 Modeling and Simulation

The Government and contractor shall establish and maintain a system for requirements definition, development, selection, control, verification, validation, and accreditation of models and simulations, techniques, tools, and outputs that are used for design and development activities and applied throughout the system life cycle in support of systems engineering activities. Modeling and simulations may be applied to support design and development activities and provide capabilities such as evaluating requirements and telemetry data, performing sensitivity and trade-off studies, performing reliability predictions, supporting design decisions, understanding and demonstrating system capabilities and performance, and exercising systems under test (3.7.8). The software used for modeling, simulating, and predicting safety and mission critical deliverable items whether developed by Government, contractor, or supplier shall be developed and controlled IAW 3.3. The MDA Directive 8315.02 provides policy and guidance for the MDA modeling and simulation program.

3.2.14.1 Verification, Validation, and Accreditation Processes

The Government's and contractor's Verification, Validation, and Accreditation (VV&A) processes shall ensure development of correct and valid simulations and provide simulation users with sufficient information to determine if the simulation can meet their needs. Verification, Validation and Accreditation processes shall be performed to establish the credibility of the models and simulations.

The Government and contractor shall ensure that the Models and Simulation (M&S) requirements are specified and included in the conceptual model. In order to accomplish this, the Government and contractor shall:

- a. Refine M&S Requirements: Results in the total set of detailed M&S requirements that the simulation needs to address.

- b. Plan M&S Development: Results in the development plan that includes information on the development approach, resource allocations, schedules, and milestones.
- c. Develop Conceptual Model: Results in the simulation conceptual model, the collection of information that describes the Government's or contractor's concept about the simulation and its constituent parts.
- d. Develop Design: Results in the design specifications, a translation of the information captured in the conceptual model to support their implementation in software (code) and hardware.
- e. Implement and Test: Realizes the design in hardware and software (code). Both hardware and software are built, integrated, and tested; and actual data and databases are installed and tested.

3.2.14.2 Models and Simulations Verification & Validation

All models and simulations used by the Government or contractor to predict the performance of MDA products shall undergo the following verification and validation activities:

- a. Verify M&S Requirements: Confirm that the requirements for the simulation match those needed for the current problem, and are correct, consistent, clear, and complete.
- b. Develop Verification & Validation (V&V) Plan: The V&V Plan shall be prepared IAW MIL-STD-3022.
- c. Validate Conceptual Model: Confirm that the capabilities indicated in the conceptual model embody all the capabilities necessary to meet the requirements.
- d. Verify Design: Determine that the design accurately reflects the conceptual model, and contains elements necessary to provide needed capabilities without adding unneeded capabilities.
- e. Verify Implementation: Determine that the code is correct and is implemented correctly on the hardware.
- f. Validate Results: Determine the extent to which the simulation addresses the requirements of the intended use.

3.2.14.3 Models and Simulations Accreditation

All models and simulations used by the Government or contractor to predict MDA performance shall undergo an accreditation process to determine that a simulation and its associated data are capable and appropriate for use in the specified application. Ballistic Missile Defense system models and simulations, as defined in MDA Directive 8315.01, shall be accredited by MDA/DE. The cognizant MDA Program Office(s) or designated representative(s) shall accredit models and simulations associated with their products. The accreditation process shall include the following:

- a. Develop Accreditation Plan: The accreditation plan shall be prepared IAW MIL-STD-3022.
- b. Collect and Evaluate Accreditation Information: The information needed for the assessment is collected from the V&V effort and other sources (e.g., product design, product test, configuration management, and risk management), and evaluated to determine its completeness.
- c. Perform Accreditation Assessment: The fitness of the simulation shall be assessed using evidence collected from the V&V effort and other sources (e.g., hardware and software qualification, and M&S developer's metrics), and an accreditation report with recommendations is prepared.

3.2.14.4 Accreditation Decision

The Government's accreditation process shall result in one of the following decisions for models and simulations used to predict MDA performance:

- a. Full accreditation: The simulation produces results that are sufficiently credible to support the application.
- b. Partial accreditation: The simulation includes caveats and limitations impacting test objectives and confidence in stakeholder analysis results. This partial accreditation may allow entrance to developmental testing with known caveats and limitations, but may prevent entrance to operational testing.
- c. Limited or conditional accreditation: Constraints should be placed on how the simulation can be used to support the application.
- d. Modification of the simulation is needed: The simulation's capabilities are insufficient to support either full or conditional accreditation; modifications and subsequent V&V are needed to correct the deficiencies.
- e. Additional information is needed: The information obtained about the simulation is insufficient to support either full or conditional accreditation; additional information should be generated or otherwise obtained, supplemental verification, validation and/or testing should be conducted to provide the necessary information before the accreditation decision is made.
- f. No accreditation: The assessment results demonstrate the simulation does not adequately support the application.

3.2.14.5 Verification, Validation, and Accreditation Documentation

The Government's and contractor's VV&A documentation shall be prepared IAW MIL-STD-3022. The cognizant MDA Program Office's VV&A documentation shall be submitted to MDA/DE for approval per MDA Directive 8315.01. The contractor's VV&A documentation shall be submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.2.15 Classification of Characteristics

The contractor shall establish and maintain a system to analyze the design to identify and classify characteristics of the product, which could affect Coordination, Life, Interchangeability, Function, and Safety. Characteristics that must be controlled, maintained, and appraised to ensure design integrity, and are deemed essential for Government acceptance requirements, shall be identified and classified in design disclosure documentation and applicable technical documentation.

3.2.15.1 Classification of Characteristics Levels

These classification levels shall be used:

- a. Critical: A critical characteristic is one that analysis indicates is likely, if defective, to create or increase a hazard to human safety, or to result in failure of a weapon system or major system to perform a required mission.
- b. Major: A major characteristic is one that analysis indicates is not critical but is likely, if defective, to result in failure of an end item to perform a required mission.
- c. Minor: A minor characteristic is one that analysis indicates is significant to product quality but is not likely, if defective, to impair the mission performance of the item.

The contractor shall:

- a. Develop a policy that delineates criteria for determining the level of test, inspection, or control to be applied to each classification level (critical, major, or minor).
- b. Base classification solely on impact to the product if the characteristic is not within specified limits and not on magnitude of the characteristic's tolerance.
- c. Identify critical and major characteristics on the drawing(s) or specification(s), or via an alternate method approved by the cognizant MDA Program Office or designated representative(s).
- d. Complete classification of characteristics before establishing each successive baseline for the system or product.

3.2.16 Electromagnetic Environmental Effects Design and Verification

The Government and contractor shall ensure the system is designed to be electromagnetically compatible among all subsystems, ordnance, equipment, and parts within the system and to be survivable and compatible with environments caused by electromagnetic effects external to the system. Electromagnetic environmental effects operational and design requirements compliance shall be verified IAW MIL-STD-464 through test, analysis, or a combination of both. Verification shall also address all acquisition process aspects of the system, including normal in-service operation, maintenance, aging, checkout, storage, transportation, handling, packaging, loading/unloading, and launch. Electromagnetic environmental effects shall encompass all applicable electromagnetic disciplines such as electromagnetic compatibility; electromagnetic interference; electromagnetic pulse; hazards of electromagnetic radiation to ordnance, fuel, and personnel; electrostatic discharge; and direct current magnetics.

3.2.17 Space Radiation, Nuclear Hardness and Survivability Program

When vulnerability requirements require the weapon system to survive radiation environment, the contractor shall establish and maintain a hardness assurance, maintenance, and surveillance program that addresses all life cycle phases. The program shall enable the system to operate in hostile environments, natural space radiation environments, and other nuclear radiation environments expected to be encountered during performance of a mission.

The contractor shall ensure Hardness Critical Items (HCI) are identified and tracked throughout the acquisition process and any changes in fabrication and production processes and materials are evaluated to ensure no radiation hardness degradation has occurred.

The Government, contractors, and Department of Energy laboratories shall implement the hardness critical test, inspection, and hardness assurance processes during assembly, production, maintenance, storage, and shipping of HCIs.

The contractor shall identify and perform periodic test and inspection of HCIs.

The program shall be coordinated with systems engineering and the Parts, Materials, and Processes Control Board (MDA-QS-003-PMAP, paragraph 2.2)

3.2.18 Transition to Operations or Production

The contractor shall plan and design for transition to operations or production throughout the development process. Planning for transition shall begin early in the system development and demonstration phase. The contractor shall ensure production disciplines and processes required for operations or production are developed concurrently with the product's design.

The Government and contractor shall use the risk management process (3.1.6) to minimize risks associated with transitioning designs to operations or production. The Government and contractor shall perform incremental risk assessments to identify and mitigate transition risk to support fielding of new or upgraded designs and production milestone decisions. The transition risk assessment shall include transition risks identified at safety and mission critical suppliers. The Government and contractor shall identify and report any remaining transition risks during Preliminary Design Reviews (3.4.1.7), Critical Design Reviews (3.4.1.8), System Verification Reviews (3.4.1.10), and Production Readiness Reviews (3.4.1.12). The risks associated with transitioning shall be effectively communicated to the cognizant MDA Program Office, MDA/DE, and MDA/QS.

3.2.18.1 Transition to Production Plan

The contractor shall establish and maintain a Transition to Production Plan, which defines the approach for supporting operations or production decisions. The plan shall address transition activities using Production Readiness Reviews (3.4.1.12), Engineering Readiness Reviews, and Manufacturing Readiness Reviews in accordance with MDA Instruction 5010.24-INS or an MDA approved alternative transition to operations or production technical risk management process. The Transition to Production Plan shall be developed concurrently with product design and stored in IDE (3.1.5).

3.2.19 Legacy Designs

Legacy or heritage designs (i.e., hardware, software, or firmware) may be used in MDA systems, subsystems, or assemblies, if the designs meet or exceed end item requirements. When used in identical applications, the Government or contractor shall provide, as a minimum: the technical data package, design validation and verification records, reliability records, and qualification records. The cognizant MDA Program Office shall approve legacy designs before incorporation into the design baseline.

For applications that are less than identical, the contractor shall perform design and risk analyses to determine the extent legacy designs shall be characterized through verification, validation, and qualification. Designs for less than identical applications shall be qualified IAW 3.3.2.7 and 3.7.3.

3.2.20 BMDS Technical Core Standards

The Government shall use BMDS technical core standards in accordance with MDA Directive 4122.01, Ballistic Missile Defense System Technical Core Standards. BMDS core standards are to be used during the entire BMDS system life cycle, including concept, design, and development, implementation, operations, sustainment, tests, and decommissioning. Core Standards are distinct from, but may be used in conjunction with, other standards. The BMDS Technical Core Standards Management Handbook, M-2699-1.0, provides guidance for technical core standards activities, including requests for variances and/or alternate standards.

The contractor shall establish and maintain a system for using BMDS Technical Core Standards, with design consideration given to the entire system life cycle. Each requirement contained in the system specification, subsystem specifications, equipment specifications, software/firmware requirements specifications, interface control documents, coordination drawings, and this document shall be considered when designing the system.

3.2.21 Safety and Mission Critical Computing Systems

The contractor's design of safety and mission critical computing systems shall comply with the following requirements and those of 3.3 and 3.14.

3.2.21.1 Computer System Synchronization

The Government or contractor shall ensure operating frequencies of processors, buses, and input/output devices are compatible with all other components and communications equipment during all test and operational environments. The Government's or contractor's design shall preclude over clocking of

Central Processing Units (CPU). The Government or contractor shall implement maximum allowable instruction execution time restrictions and ensure buses and input and output devices provide instructions and data at an acceptable rate. The Government or contractor shall test system performance at CPU and memory utilizations rates at 2.0 times the highest values predicted for operations.

3.2.21.2 Read-Only Memories

The Government's or contractor's design of computing systems where Read-Only Memories are used shall include measures to ensure memory contents will not cause a software or system fault if corrupted.

3.2.21.3 Self-Checking Design Requirements

The Government's or contractor's design of computing systems and safety and mission critical applications shall meet self-checking requirements in [3.2.21.3.1](#) and [3.2.21.3.2](#).

3.2.21.3.1 Time Constraints for Execution

The Government or contractor shall design computing systems to execute within predefined time limits such that failures to complete a task as scheduled are identified, the operator is alerted, and the system provides the capability to return to a known safe state. The system shall include:

- a. Safety and mission critical functions, which require rapid response (beyond expected human cognitive response and reaction) shall be controlled by a computer and not rely on human input. Timing values for safety and mission time critical function execution shall not be modifiable by the operator.
- b. When in an operational mode, automated responses to failures shall not impede ongoing operations.
- c. Recursive and iterative loops shall have a maximum documented execution time. Checks shall be performed to prevent loops from exceeding maximum execution time.
- d. Safety and mission critical routines in real time programs shall ensure data used is still valid.

3.2.21.3.2 Memory Checks

The Government's or contractor's design shall include periodic checks of memory and each data bus to ensure failures are detected and mitigated. Checksum of data transfers and Program Load Verification checks shall be performed at load time and periodically thereafter to ensure integrity of safety critical code.

3.2.21.4 Systems Degradation

The Government or contractor shall design the system and software to prevent degradation of safety or mission critical functions by other interfacing automata and software.

3.2.21.5 Unauthorized Interaction

The Government or contractor shall design the system to prevent unauthorized system or subsystem interaction from initiating or sustaining a safety or mission critical function sequence.

3.2.21.6 Unauthorized Access

The Government's or contractor's system design shall prevent unauthorized or inadvertent access to, or modification of, the software (source, assembly, and object code) and firmware. This includes preventing self-modification of the code.

3.2.21.7 Peak Load Requirements

The Government or contractor shall design the system to ensure design safety requirements are not violated under peak load conditions. Central processing units (CPU), firmware devices, and memory shall be designed to a safety factor of no less than 2.0 times the maximum expected load. Buses, networks, and software, shall be designed to a safety factor of no less than 1.5 times the maximum expected load.

3.2.21.8 Fault Tolerance

The Government's or contractor's computer system architecture shall be dual failure/fault tolerant.

3.3 Software and Firmware

The Government and contractor shall establish and maintain a system to implement software and firmware requirements as specified herein. These requirements are mandatory for all deliverable safety and mission critical software, all software used to accept safety and mission critical deliverable items, and software used for modeling, simulating, and predicting performance of safety and mission critical deliverable items whether developed by Government, contractor, subcontractor, or supplier. Those requirements applicable to firmware are annotated below and specific firmware requirements related to hardware are addressed in [3.3.4](#). The integration of computer instructions and data onto a firmware device are addressed in [3.3.3.11.6](#).

These requirements apply to Commercial-Off-The-Shelf (COTS) and Non-Developmental Items (NDI) software, auto-generated code, and reused code that is safety or mission critical, or that has a direct impact on, or association with, safety critical hardware or a safety critical function.

3.3.1 Management Processes

The Government and contractor shall implement software management and infrastructure processes that are based on industry software best practices (e.g., IEEE 12207, Capability Maturity Model Integration (CMMI) for Development), and are IAW SAE AS9100, MAP Provision [3.1](#), and these requirements:

- a. Government's and contractor's program manager shall ensure a software project manager is designated for each software project.
- b. Government's and contractor's software project manager shall ensure assigned projects are planned, managed, tracked, controlled, and reported.
- c. Government's and contractor's software project managers shall be responsible for negotiating commitments and developing, documenting, and implementing the software development plan, software projects activities, products, and results.

3.3.1.1 Intergroup Coordination

Contractor's software engineering shall participate with other engineering groups, safety, end users, and MDA in establishing system requirements, performing requirements allocation, and making design trade-offs ([3.2.4](#)).

3.3.1.2 Software Development Plan

The Government and contractor shall use requirements allocated to software as the basis for planning software design, development, test, and supporting activities. The planning shall be documented in a Software Development Plan (SDP).

The SDP shall define the project's developmental model, tasks, activities, and products. For each development phase and activity, the SDP shall identify entry and exit criteria. The SDP shall identify software products that are required and their associated controls. The SDP shall define the approaches and methods for tracking and reporting activities, tasks, and progress and shall address the following planning activities:

- a. Software estimations for cost, schedule, effort, and resources.
- b. Project organizational structure, authority, and responsibility of each organizational unit, including external interfaces and both internal and external stakeholders.
- c. Work breakdown structure.
- d. Software products that undergo review or inspection.

- e. Methods and tools to be used for design and development, requirements analysis, software safety (3.14.9), coding (3.3.2.3.1), verification, validation, testing, configuration management (3.3.3.11), and software assurance.
- f. Engineering environment (for development, operation, or maintenance, as applicable), including test environment, library, equipment, facilities, standards, processes, procedures, and tools.
- g. Identification of all proposed subcontracts, Government Furnished Equipment (GFE), Government Furnished Information (GFI), COTS, legacy, third party, and NDI software; and address how the software is to be used and its applicable controls.
- h. Identification of software model based tools approved for use.
- i. Guidelines and criteria for tailoring the organization's standard software processes.
- j. Identification of requirements and guidelines for establishing and maintaining software process databases.

The SDP shall define the method used to ensure: the development environment is available to software developers and other users before the start of each development phase, the development team has experience or training in applying tools and methods, and tools are under configuration control.

The SDP shall include the proposed verification and validation activities for all safety, quality, functional, and performance requirements, including the approach for interfacing with the Independent Verification and Validation (IV&V) agent.

The SDP and all updates shall be submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. The SDP shall be maintained consistent with current project requirements. The contractor shall maintain records of all software planning and re-planning efforts and data.

3.3.1.3 Estimation

The contractor shall establish and maintain a system for estimating resource requirements for software projects and products. The system shall address:

- a. Software scheduling efforts, including critical dependencies and critical paths.
- b. Software product size and complexity.
- c. Software effort and costs.
- d. Critical computer resources (e.g., input/output, buffer, and memory).

The contractor's estimations shall be used as inputs to the planning process. Records of estimations shall be maintained for future use and reference.

3.3.1.4 Software and Firmware Risk Management

The Government's and contractor's risk management process shall identify software and firmware risks IAW 3.1.6 and include:

- a. Tracking risks throughout the MDA system life cycle.

- b. Corrective actions for deviations from the mitigation plan.
- c. Watch list for all low risks, which shall be periodically re-assessed.

3.3.1.5 Software Process Improvement

The Government and contractor shall establish and maintain a software improvement process for developing, assessing, measuring, controlling, reporting, and improving software processes.

The software improvement process shall address:

- a. Organizational processes for all software development and maintenance activities. The processes and their application to specific cases shall be documented.
- b. Process assessments and required records.
- c. Improvements to organizational processes as a result of process assessment and review. The contractor shall update process documentation to reflect improvement in organizational processes.
- d. Standards for documenting software processes and improvements.
- e. Coordination of software process databases.
- f. Monitoring, evaluating, introducing, or transferring new processes, methods, and tools into the organization.
- g. Collecting, analyzing, maintaining, reporting, and using software quality data to support process assessments and improvements.
- h. Communication of software process development, maintenance, and improvement activities within the organization.

The Government and contractor shall establish and maintain a system for performing quantitative process management activities. Measurement data shall be collected and analyzed and software processes brought under quantitative control. Results of activities shall be documented and distributed to affected organizations. Quantitative measurement activities shall be used to establish process capability baselines.

3.3.1.6 Software and Firmware Supplier Management

The contractor shall use the supplier management program for selection of software and firmware suppliers and management of software and firmware subcontracts. Requirements of this section supplement those of SAE AS9100 and [3.13](#), Supplier Management. Before contract award, the contractor shall inform the cognizant MDA Program Office of all safety and mission critical software and firmware supplier selection decisions.

3.3.1.6.1 Flow Down of Requirements

The contractor shall flow down requirements IAW [3.13.4](#), Supplier Program Requirements.

3.3.1.6.2 Acceptance of Supplier Software and Firmware Products

Supplier product acceptance by the contractor shall be accomplished IAW approved plans and procedures addressing quality, safety, functional, performance, load, interoperability, and stress testing requirements. Acceptance shall also include review and approval of all operational and maintenance documentation.

3.3.1.7 Software Personnel Training

The Government and contractor shall ensure software managers, software engineers, Software Quality Assurance (SQA) personnel, configuration management personnel, and other related groups are adequately trained to implement tasks and activities required.

Personnel performing SQA and Software Configuration Management (SCM) functions shall be trained to perform their activities, while other members of the software project shall receive orientation on roles, responsibilities, and value of SQA.

Software managers, software engineers, and other individuals participating in project planning shall be trained in software estimating and planning procedures applicable to their area of responsibility. Software managers shall be trained in managing technical, administrative, and personnel aspects of a software project.

Individuals responsible for developing the project's software processes shall receive required training in how to tailor the organization's standard software processes.

3.3.2 Software Development, Maintenance, and Operational Processes

The contractor shall establish and maintain specific standards, methods, tools, actions, and responsibility associated with development, qualification, and maintenance of all requirements including a method for identification and tracking of safety related requirements.

Non-deliverable items may be employed in development or maintenance of the software product; however, the contractor shall ensure operation and maintenance of the delivered software is independent of such items; otherwise those items shall be considered as deliverable.

3.3.2.1 Requirements

The contractor's system requirements analysis and allocation process shall:

- a. Establish and maintain requirements allocated to software and firmware. Safety and mission critical functional requirements shall be reviewed to ensure they are complete, feasible, clearly stated, consistent, and verifiable. Problems noted with allocated requirements shall be documented and resolved with responsible parties. Bi-directional traceability shall be established from the source requirement down to its implementation level requirements and from the implementation level requirements back to the source. Changes to allocated requirements shall be reviewed, approved, and incorporated into the project IAW documented processes and procedures.
- b. Flag or uniquely identify software/firmware safety and mission critical item requirements and characteristics affecting coordination, life, interface, and functional requirements ([3.2.15](#)).
- c. Select and use operating systems, standard languages, architectures, and tools, which provide for open systems ([3.2.13](#)).
- d. Evaluate systems software and firmware requirements to assess the following:
 - 1) Identification of software and firmware requirements which are safety and mission critical.
 - 2) System requirements have been appropriately allocated to software items, firmware items, and manual operations according to design criteria.
 - 3) Software and firmware requirements accurately reflect system requirements.
 - 4) Feasibility of software and firmware items fulfilling their allocated requirements.

Results of the evaluation shall be documented and maintained as a quality record and stored in IDE [\(3.1.5\)](#).

3.3.2.1.1 Software Reuse

The contractor shall evaluate reusable software products to determine if they meet specific MDA program requirements and are cost effective over the life of the system. Reused software includes previously developed software, which is used for project development as is or with adaptation. This includes COTS software, and software supplied by the Government (i.e., GFI and NDI).

The contractor's analyses of existing software shall be carried out and finalized at the architectural design stage. The contractor shall provide evidence of the product's suitability. This evidence includes an assessment of the relationship between the software's original intended environment and the proposed environment, impact of any differences on the software performance, and impacts of known defects on safety and mission requirements. When analysis of available data indicates risks, the contractor shall propose and obtain agreement on additional verification tasks to be performed from the cognizant MDA Program Office or designated representative(s). The basis for reuse decisions shall be documented and maintained.

Before incorporation into the product baseline, the contractor shall submit software reuse documentation into IDE [\(3.1.5\)](#) for review and concurrence by the cognizant MDA Program Office. Reused software shall be subject to the same requirements as newly developed software.

3.3.2.2 Software Design

The contractor shall ensure software design is developed, maintained, documented, and verified per software specifications and SDP. The software design shall be traceable to software requirements and form the architecture framework for coding. Software design products shall be consistent with software requirements, software code, and project requirements. The software design specification or model shall define the architecture, variable control, variable range, modularity, parameter ranges, parameter designations, and complete logic flow for all processing. Software flow charts or models shall include all decision paths, decision logic, complex algorithms by mathematical formula, parameter designations, parameter lookup tables, explanations of unique code associated with input/output, and explanations of unique code associated with how data schema are generated. For object oriented design, this includes inventory of classes, verification of methods, class hierarchy, and schema validation. Software technical documentation shall also identify those algorithms directly affecting system performance and shall provide a verification matrix designating status on whether algorithms have been qualified and verified. Contractor's design and evaluation activities shall include:

- a. Definition and documentation of test requirements and schedule for testing software units. Test requirements shall include stressing the software unit.
- b. Development of operation and maintenance documentation. Preliminary or draft versions of the documentation shall be available at the Critical Design Review [\(3.4.1.8\)](#) for review and comment by end users, the cognizant MDA Program Office and designated representative(s). Documentation shall be updated based upon feedback from reviewers. Contractor's final operation and maintenance documentation presented for Government acceptance shall define delivered capabilities and limitations.
- c. Review of software design requirements to assess:
 - 1) Proper sequence of events, inputs, outputs, interfaces, logic flow, allocation of timing and sizing budgets; and error definition, isolation, and recovery.
 - 2) Selected design can be derived from requirements.

- 3) Complete and accurate implementation of safety and mission critical requirements.
- 4) External consistency with architectural design.
- 5) Internal consistency between software components and software units.
- 6) Appropriateness of design methods and standards used.
- 7) Traceability to requirements of the software item.
- 8) Feasibility of testing, operation, and maintainability.
- 9) Review results shall be documented and maintained as a quality record and stored in IDE ([3.1.5](#)).

d. Appropriateness of programming language features, constructs, limitations, and methods used.

3.3.2.3 Software Code/Implementation

The contractor shall ensure software is developed, maintained, documented, and verified. Code/Implementation shall be traceable to software design. Software code/implementation shall be documented and include comments IAW coding standards. Use of language features shall be IAW specific guidelines and safety limitations ([3.14](#)). There shall be no undocumented features in the code/implementation. Software code/implementation shall be maintained consistent with software design and project requirements.

3.3.2.3.1 Software Programming Standards

Programming standards shall address:

- a. Assignment Statement: Mission or Safety Critical Computing System Functions ([3.14.7](#)) and other safety or mission critical software items shall not be assigned values using non-mission critical or non-safety critical sources.
- b. Automatically Generated Code: Before use, tools used for automatically generating code shall be documented to include the following data: use, limitations, acceptable and unacceptable output, manufacturer, and version. A certificate of compliance shall be submitted to the IDE ([3.1.5](#)) for review and concurrence by the cognizant MDA Program Office or designated representative(s).
- c. Compilers: Software compilers shall be validated to ensure compiled code is fully compatible with the target computing system and application (i.e., may be done once for a target computing system). Compilers shall not be resident on the target system.
- d. Deactivated Code: Contractor shall ensure deactivated code is disabled for environments where its use is not intended. The contractor shall perform a coverage analysis and test that demonstrates the means by which code may be inadvertently executed are eliminated.
- e. Dead Code: Contractor shall ensure software shall not contain dead code for which the software control structure never allows execution.
- f. Fault Detection: Fault detection and isolation programs shall be written for safety and mission critical subsystems of the computing system. The fault detection program shall be designed to detect potential critical failures before execution of related safety ([3.14.11.3.6](#)) and mission critical function. Fault isolation programs shall be designed to isolate the fault and provide fault information to the operator or maintainer.

- g. Indirect Addressing: When used, the address being pointed or re-directed to, shall be verified as acceptable before being referenced.
- h. Safety and Mission Critical Files: Files used to store or transfer safety or mission critical information shall be initialized to a known state before and after use. Data transfers and data stores shall be audited, where practical, to allow traceability of system functioning.
- i. Operating System Functions: Operational programs shall only use operating system functions that are provided.
- j. Overlays: Overlays of safety and mission critical software shall all occupy the same amount of memory. Where less memory is required for a particular function, the remainder shall be filled with a pattern that, if executed, will cause the system to revert to a safe state. It shall not be filled with random numbers, halt, stop, no-op, or wait instructions or data from previous overlays.
- k. Single Purpose Files: Files used to store safety or mission critical data shall be unique and have a single purpose. Scratch files, those used for temporary storage of data during or between processes, shall not be used for storing or transferring safety or mission critical information, data, or control functions.
- l. Unused Memory: All processor memory not used for or by the operational program shall be initialized to a pattern that, if executed, will cause the system to revert to a safe state. It shall not be filled with random numbers, halt, stop, wait, or no-op instructions. Data from previous overlays or loads shall not be allowed to remain.
- m. Test Code: Code utilized for specific test purposes, test scenarios, or analysis shall only remain within the software if it has been planned and targeted for further use and utilization in the software beyond formal release.
- n. Fault Tolerance: Contractor's software design shall ensure dual fault tolerance against the failure of safety or mission critical software functions.

3.3.2.3.2 Software Coding Standards

The contractor's coding standards shall address:

- a. Conditional Statements: Conditional statements shall have all possible conditions satisfied and under full software control (i.e., there shall be no potential unresolved input to the conditional statement). Conditional statements shall be analyzed to ensure conditions are reasonable for the task and that all potential conditions are satisfied and not left to a default condition. All conditional statements shall be annotated with their purpose and expected outcome for given conditions.
- b. Flags and Variables: Flags and variable names shall be unique. Flags and variables shall have a single purpose and shall be defined and initialized before use.
- c. Loop Entry Point: Use of loops shall be restricted to only one entry point. Branches into loops shall not be used. Branches out of loops shall lead to a single exit point placed after the loop within the same module.
- d. Modular Code: Software design and code shall be modular. Modules, including methods, subroutines, and similar executable code objects, shall have one entry and one exit point.
- e. Software Maintenance Design: Software shall be annotated, designed, and documented for ease of analysis, maintenance, and testing of future changes to the software.

- f. **Timer Values Annotated:** Values for timers shall be annotated in the code. Comments shall include a description of the timer function, its value, and rationale or a reference to the documentation explaining the rationale for the timer value. These values shall be verified and examined for reasonableness for the intended function.
- g. **Uninterruptible Code:** If interrupts are used, sections of code, which have been defined as uninterruptible, shall have defined execution times monitored by an external timer.
- h. **Unnecessary Features:** Operational and support software shall contain only those features and capabilities required by the system requirements. The programs shall not contain undocumented or unnecessary features ([3.3.2.4](#)).
- i. **Unused Executable Code:** Operational program loads shall not contain unused code (Functionality which may be needed in a later version shall be commented out or otherwise eliminated before compilation).
- j. **Variable Declaration:** Software variables or constants used by safety or mission critical functions will be declared/initialized at the lowest level (e.g., unit, function, or object).

The related coding standard and requirements shall be consistent with type, size, complexity, intended use of the system and its intended environment (additional safety coding standards in [3.14.9.1](#)).

3.3.2.3.3 Software Code Analysis

Contractor shall perform software code analysis to verify the coded program correctly implements the verified design and does not violate quality, safety, and mission assurance requirements. The contractor shall:

- a. Perform code data analysis on data structures and usage on internal application data. Data analysis shall determine how data items are defined and organized and ensure these data items are consistently defined and used.
- b. Perform code logic analysis and evaluate the sequence of operations represented by the program to detect logic errors in software.
- c. Perform code interface analysis to verify compatibility of internal and external interfaces. This analysis shall verify parameters are properly passed across interfaces.
- d. Perform interrupt analysis to determine how interrupts are used by software. Contractor shall ensure:
 - 1) Interrupts cannot lead to priority inversion and prevent a high priority or safety critical task from completing.
 - 2) Undefined interrupts are received and processed, such that interrupts do not cause program failures.
 - 3) Time critical events are executed within time constraints.
 - 4) Timing critical areas are protected from interrupts, if a delay would result in unacceptable behavior.
 - 5) Interrupts inhibited for a period of time shall be buffered by the system for this period to prevent the loss of interrupts.
- e. Ensure code is traceable to design and requirements, testable, verifiable, and compliant with requirements and coding standards.

- f. Ensure code implements proper event sequence; consistent interfaces; correct data and control flow; appropriate allocation timing and sizing budgets; and error definition, isolation, and recovery.
- g. Perform formal inspections on safety and mission critical software components.
- h. Verify that code can be derived from design or requirements.
- i. Ensure external consistency with interface requirements and design of the software item.
- j. Ensure internal consistency between unit requirements implementation.
- k. Ensure test coverage of units ([3.3.2.4](#) and [3.3.2.5](#)).
- l. Ensure appropriateness of programming language features, constructs and limitations, coding methods, and standards used.
- m. Ensure feasibility of software integration ([3.3.2.6](#)) and testing ([3.3.2.7](#)) according to the integration/build plan and test plan.
- n. Ensure feasibility of operation ([3.3.2.14](#)) and maintenance ([3.3.2.15](#)) of the product.

Results shall be documented and maintained as a quality record and stored in IDE ([3.1.5](#)).

3.3.2.4 Software Test Coverage and Analysis

The contractor shall establish and maintain a system to manage software test coverage and analysis. Computer based tools shall be used to ensure coverage is complete. Software test coverage efforts shall include analyses identified herein, and shall be applied to software unit, software integration, and system level testing. Software testing shall include:

- a. Go-No-Go path testing.
- b. Hardware and software failure mode testing to verify systems fail into a safe state.
- c. Boundary, out-of-bounds, and boundary crossing test conditions.
- d. Minimum and maximum input data rates in worst case configurations to determine the system's capabilities and responses to these conditions.
- e. Denominator values of zero, zero crossing, and approaching zero from either direction or similar values for trigonometric functions.
- f. Regression testing when changes are made that may impact safety and mission critical computing system functions.
- g. Operator interface testing with introduction of operator errors during safety and mission critical operations to verify safe system response to these errors.
- h. Duration stress testing. Testing shall be conducted under simulated operational environments. Additional stress duration testing should be conducted to identify potential critical functions (e.g., timing, data senescence, and resource exhaustion) that are adversely affected as a result of operational duration. Software testing shall include throughput stress testing (e.g., CPU, data bus, memory, and input/output) under peak loading conditions.

3.3.2.4.1 Requirements Based Test Coverage Analysis

The contractor shall perform a software requirements based test coverage analysis to determine how well requirements based testing verified implementation of software requirements. This analysis shall identify any need for additional requirements based test cases. The requirements based test coverage analysis shall demonstrate that adequate test cases exist for each software requirement.

3.3.2.4.2 Structural Test Coverage Analysis

The contractor shall perform a structural test coverage analysis to determine if any code structure was not exercised by requirements based test procedures. The contractor shall perform additional software testing when structural coverage analysis reveals that a code structure was not exercised during requirement based testing.

3.3.2.4.3 Software Threading and Concurrency Analysis

The contractor shall perform analyses that demonstrate safe use of threading and concurrency when used as part of software design (i.e., threading shall not result in data conflicts or deadlocks). Analysis shall include:

- a. Code verification to ensure functions are thread safe.
- b. Verification that objects are fully initialized before allowing access.

3.3.2.4.4 Multitasking and Multicore Processing Analysis

The contractor shall perform analyses to identify conditions leading to deadlocks, data conflicts, resource conflicts, or resource and timing issues in systems utilizing threading, multitasking, multicore processors, or multiple processors.

3.3.2.5 Software Unit Testing

The contractor shall perform unit testing to demonstrate software design has been successfully implemented in the software code. Unit test criteria (inputs, expected results, evaluation, and acceptance criteria) shall be developed to specify types of test cases that are to be executed. Test cases shall cover the unit's design.

- a. Unit testing for safety or mission critical software shall be performed to:
 - 1) Detect errors in translation of design requirements into code prior to integration with other computer software units.
 - 2) Detect errors in algorithms and logic used to implement software requirements and design specifications.
 - 3) Verify each computer software unit fully satisfies applicable software requirements and design specifications.
 - 4) Detect and eliminate all unused, unreachable, or unexecutable code.
 - 5) Ensure all statements and decisions are executed.

Unit testing results shall be documented and maintained as quality records and stored in IDE [\(3.1.5\)](#). Defects shall be recorded and tracked to closure. Unit test results shall certify software code has been compiled error free and that it successfully passed all unit tests.

- b. The contractor shall evaluate software unit test results to assess the following:

- 1) Traceability to requirements and design of software item.
- 2) External consistency with requirements and design of the software item.
- 3) Internal consistency between unit requirements.
- 4) Test coverage of units.
- 5) Appropriateness of coding methods and standards.
- 6) Feasibility of software integration and testing.

Evaluation results shall be documented and maintained as a quality record in IDE ([3.1.5](#)).

3.3.2.6 Software Integration Testing

The contractor shall plan and perform software integration testing. Integration testing shall verify software code implements design and interface requirements specified in design documentation at unit, component, and Software Configuration Item (SCI) level. Test cases shall cover SCI architectural design. When applicable, software integration testing shall assure adequacy of human-machine interfaces. All problems or issues identified during integration testing shall be documented and tracked to resolution ([3.3.3.8](#)). Problems or issues associated with software safety shall be reported IAW [3.14](#). Results of software integration testing shall be collected, analyzed, reported, and maintained in IDE ([3.1.5](#)).

The contractor shall evaluate the integration plan, design, code, tests, test results, and user documentation to assess the following:

- a. Software components and units of each software item are completely and correctly integrated.
- b. Traceability to system requirements.
- c. External consistency with system requirements.
- d. Internal consistency between software and documentation.
- e. Test coverage of software item requirements.
- f. Appropriateness of test standards and methods used.
- g. Conformance to expected results.
- h. Feasibility of software qualification testing.
- i. Feasibility of operation and maintenance.

Evaluation results shall be documented and maintained as a quality record in IDE ([3.1.5](#)).

3.3.2.7 Software Qualification

The contractor shall plan and perform software qualification. Software qualification shall validate the SCI and integration of SCIs to ensure they meet allocated software requirements. Software qualification cases and procedures shall be planned, prepared, and executed by personnel independent from those responsible for the item's design and implementation (code). Test cases shall be traceable to individual software requirements. Software qualification shall be performed against allocated software requirements. Results of software qualification shall be collected, analyzed, reported, and maintained.

Operations and maintenance documentation shall be proofed or qualified during software qualification testing. All problems or issues identified during software qualification shall be documented and tracked to resolution ([3.3.3.8](#)). Safety problems, issues, or deficiencies shall be clearly identified and reported IAW [3.14](#).

Contractor's software qualifications shall:

- a. Ensure implementation of each software requirement is tested for compliance.
- b. Be performed at the highest level of integration practicable, using intended system hardware documentation, and actual operating conditions to the highest degree practicable. Qualification testing shall demonstrate all interfaces are verified and user documentation is complete and correct.
- c. Consist of functional, performance, load, stress, and fault testing.
- d. Demonstrate any associated human-machine interfaces are complete and correct.

The contractor shall make available its testing facilities, application software, and support tools for independent Government testing once its software qualification is complete. The contractor and the cognizant MDA Program Office shall concur on mutually agreeable resource schedule.

3.3.2.7.1 Software Qualification Test Report

The contractor shall prepare a software test report upon completion of qualification testing. Representative(s) from the contractor's software quality and maintenance organization shall sign the report. The report shall certify conformance to the procedures and state the conclusion concerning the test result for the software product under test (accepted, conditionally accepted, or rejected). All safety problems, issues or deficiencies shall be clearly identified and reported IAW [3.14](#). The software qualification test report shall be maintained as a quality record and stored in IDE ([3.1.5](#)).

3.3.2.7.2 Software Requalification

Contractor shall re-establish software qualification when any change is made to the software. When software is changed, a qualification analysis shall be conducted not just for qualification of the individual change, but also to determine the extent and impact of that change on the entire software system. Based on documented results of this analysis, the contractor shall then conduct an appropriate level of software regression and qualification testing to show that unchanged but vulnerable portions of the system have not been adversely affected. Results of analysis and requalification testing shall be documented and maintained as a quality record and stored in IDE ([3.1.5](#)). Design controls and appropriate testing shall provide confidence that the software is qualified after a software change has been implemented.

The contractor shall perform a software requalification test when any of the following occurs:

- a. Any change that affects a safety critical or mission critical function.
- b. Any change that affects interface requirements.
- c. Previous software qualification tests have been invalidated by a system or field failure.
- d. Changes to the allocated baseline.
- e. Changes to make the software system usable in a changed or new environment.
- f. Changes made to software to improve the performance, maintainability, or other attributes of the software system.

The requirements for Software Qualification ([3.3.2.7](#)) and Software Qualification Test Reports ([3.3.2.7.1](#)) shall also apply to software requalification. These requirements supplement the Requalification Test program requirements in [3.7.3](#).

3.3.2.8 Regression Tests

The contractor shall perform regression tests for verifying changes to software once the software has successfully completed unit test. When software is changed, a regression test analysis shall be performed to determine the extent and impact of that change on the entire software system. Regression tests shall verify changes have been successfully implemented, errors have not been introduced, and software complies with specified requirements. Criteria for determining the extent of regression testing required shall be developed and available to the cognizant MDA Program Office and designated representative(s). Regression test suites shall be available to the cognizant MDA Program Office. Test results shall be stored in IDE ([3.1.5](#)). The method or process shall also ensure only approved changes have been implemented into the code.

3.3.2.9 Software Test Program Status Reports

The contractor shall prepare and distribute software test program status reports to project and program management on a monthly basis for information and action. Information from these reports shall be used as inputs to the process improvement ([3.1.4](#)) and risk management ([3.1.6](#)) programs. These reports shall include:

- a. A description of significant problems, corrective actions taken, schedules for accomplishment of planned actions, and lessons learned.
- b. Updates of test schedules.
- c. A list of all tests planned and completed during the report period, indicating whether the test objectives were met.
- d. A description and status of all defects, problems, and failures that occurred during the reporting period. Defects, problems, and failures associated with safety and mission critical items shall be highlighted.
- e. Status of previous failures, which remain open, and a description of corrective actions taken on failures closed during the reporting period.
- f. Status of all test objectives.

These test status reports shall be stored in IDE ([3.1.5](#)).

3.3.2.10 System Integration

The contractor shall integrate software and firmware configuration items with hardware configuration items, manual operations, and other systems. The aggregates shall be tested against system level requirements. Integration test results shall be documented, collected, analyzed, reported, and maintained.

The contractor shall evaluate the integrated system assuring:

- a. Hardware items, software items, firmware and manual operations of the system have been completely and correctly integrated into the system.
- b. Integration tasks have been performed IAW an integration plan.
- c. Test coverage of system requirements.

- d. Appropriateness of test methods and standards used, based upon intended system performance.
- e. Conformance to expected results.
- f. Feasibility of system qualification testing.
- g. Feasibility of operation and maintenance.
- h. All safety and mission critical functions and mitigations are completely and correctly integrated into the system.
- i. No emergent behavior exists, that adversely affects the safety or performance of the system.
- j. Abnormal inputs, operating conditions, or safety mishaps do not result in undesired behavior.

Evaluation results shall be documented, maintained, and stored in IDE [\(3.1.5\)](#) as a quality record.

3.3.2.11 System Qualification

The contractor shall support qualification of computing systems as part of the overall system qualification [\(3.7.3\)](#).

3.3.2.12 Software Installation

The contractor shall establish and maintain a plan for installation of software product and upgrades in the target environment. The resources and information necessary to install the software product shall be determined and available to MDA. The contractor shall develop the procedure for installing the software product in the target environment. Installation procedures shall be written so that an independent group can perform the installation. Safety issues relating to installation shall be clearly documented and stored in IDE [\(3.1.5\)](#). The contractor shall provide notification, at least 24 hours in advance, to ensure the cognizant MDA Program Office or designated representative(s) has an opportunity to witness software installation. The contractor shall assist the Government with installation activities as required. Where the installed software product is replacing an existing system, the contractor shall support any parallel activities.

When required, the contractor shall perform installation IAW the installation procedure. All deficiencies, problems, or issues associated with performance, capabilities, limitations, or the installation process shall be documented, reported, tracked, and resolved [\(3.1.10\)](#).

When File Transfer Protocol (FTP) is used to support software installation, the contractor shall ensure that files are transferred over a secure network and that files are received from a configuration controlled source library. File transfers shall be verified to ensure that files map to the correct configuration item and that files were not corrupted in transit.

3.3.2.12.1 Software Deliverable Package

The contractor shall identify and prepare the software and associated documentation needed to support software transition to operations and maintenance. The contractor shall update requirement [\(3.3.2.1\)](#) and design documents [\(3.3.2.2\)](#). The software deliverable package shall be submitted into IDE [\(3.1.5\)](#) and marked for approval by the cognizant MDA Program Office. Notification that the software deliverable package is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. For all version and dot builds the Software Deliverable Package shall include:

- a. Source code with build instructions including build scripts and any necessary input files: All items needed to regenerate the executable software shall be provided.

- b. Executable code: Executable software, including any batch files, command files, data files, or other software files needed to install and operate software on its target computer(s).
- c. Software documentation: Documentation (e.g., Software Version Description (SVD)) that reflects the "As-Built" software products along with support documentation. Additionally, operations and maintenance manuals (e.g., programming and firmware support manuals) shall be provided.
- d. Software installation procedures: All installation procedures for the target environment ([3.3.2.12](#)). Contractor shall demonstrate all installation procedures are accurate and complete.
- e. Installation verification methodology: Procedures or tools to verify correct installation.
- f. Software test code and instructions, if required to support software installation and verification.

3.3.2.12.2 Software Release Review

Contractor's Software Release Reviews shall be conducted for all major software builds and dot builds for all safety and mission critical software. The review shall evaluate formal qualification test results, software build documentation status, and ensure all identified test cases were executed, data analyzed, anomalies documented, and any risks were identified. Based upon review results, a software release recommendation shall be agreed upon by both the cognizant MDA Program Office or designated representative(s) and contractor. The software release review shall be conducted when all test results as well as all products specified in section [3.3.2.12.1](#) are available for review. The exit criteria are that all potential safety and mission assurance issues have been discussed and that all risks have been either mitigated or accepted by MDA.

3.3.2.13 Software Acceptance

At software acceptance the contractor shall provide objective evidence that:

- a. Deliverable software complies with the contractual requirements, including any specified content of the software acceptance data package.
- b. Deliverable products are complete and contain proper versions.
- c. Executable code was generated from configuration managed source code components and installed IAW predefined procedures on the target environment.
- d. Approved changes are implemented and verified.
- e. All discrepancies, nonconformances, open work, and variances (waivers or deviations) are properly documented, and resolved.
- f. All acceptance documentation is present, including any necessary certifications.
- g. All tools and development and build environments are available to the Government.

3.3.2.14 Operation

The contractor shall establish and maintain a plan and set of operational procedures for performing activities and tasks associated with operational testing, systems operation, and user support. These tasks and activities shall include the following:

- a. Procedures for testing software and firmware product in its operational environment.

- b. Procedure for receiving, recording, tracking problems, providing feedback on problems, and resolving problems (3.3.3.8). Problem reports may be passed to contractor or maintainer for resolution as appropriate. Problem reports and their resolutions shall be stored in IDE (3.1.5).
- c. Procedures required for providing assistance and consultation to users.
- d. Procedures for forwarding user requests, as necessary, to maintenance organization for resolution.
- e. Procedures for systems operations.

3.3.2.15 Software Maintenance

The contractor shall establish and maintain a Software Maintenance Plan and procedures IAW IEEE Standard 14764. The plan shall be verified against specified requirements for maintenance of the software product. The Software Maintenance Plan shall be submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. Software maintenance requirements for safety critical computing system applications are specified in 3.14.10.

3.3.2.16 Software Retirement

The contractor shall develop and document a software retirement plan. The plan shall address the following:

- a. Cessation of full or partial support.
- b. Archiving of the software product and its associated documentation.
- c. Responsibility for any future residual support issues.
- d. Transition to new product, if applicable.
- e. Accessibility of archived data.

All associated development documentation, logs, and code shall be placed in archives when software is retired.

3.3.3 Supporting Activities and Processes

The contractor shall establish and maintain a planned and systematic set of activities and tasks, which ensure software processes and products conform to requirements. This includes defining and implementing a software assurance program, software configuration management disciplines, and software documentation requirements. The contractor's software assurance program shall include SQA, Software Safety, Software Dependability, Software Reliability, and Software Verification and Validation disciplines.

3.3.3.1 Software Quality Assurance Plan

The contractor shall establish and maintain a SQA Plan for conducting the software quality assurance activities and tasks IAW IEEE Standard 730 and 730.1. The SQA plan and subsequent updates shall be submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. Records of quality assurance activities and tasks shall be stored in IDE (3.1.5).

3.3.3.2 Software Verification

The Government and contractor shall plan and accomplish verification of safety, quality, functionality, and performance requirements allocated to software. Contractor shall select a qualified organization responsible for conducting the verification effort. This organization shall be vested with authority and independence necessary to perform this task.

- a. The contractor at each life cycle stage shall ensure:
 - 1) Planned verification activities are adequate to determine products are compliant with requirements and specifications.
 - 2) Verification activities are performed using methods, procedures, and tools defined in the SDP and SQA Plan.
 - 3) Verification of all safety and mission critical software.
 - 4) Bi-directional traceability matrices are updated, verified, and complete.
 - 5) Acceptance criteria for moving forward to subsequent stages are defined and documented.
 - 6) Identification of product characteristics crucial to its safe and proper functioning.
- b. The contractor shall verify outputs of each development stage for conformance against inputs to that phase and demonstrate conformance to appropriate development standards.
- c. The contractor shall ensure verification results, including any problem reports and any corrective actions against specified requirements, are met, recorded, and verified.

The contractor shall document verification activities and results and store in IDE ([3.1.5](#)).

3.3.3.3 Software Validation

Government and contractor software validation shall ensure all software products comply with all documented software and system requirements. The correctness and completeness of both system requirements and software requirements shall be addressed as part of the design validation process ([3.2.11](#)). Government and contractor software validation shall include confirmation of conformance to all software specifications and confirmation that all software requirements are traceable to system specifications for its intended operating environment.

The contractor's validation organization shall be vested with authority and independence necessary to perform this task. The contractor shall ensure the organization responsible for validation tasks establishes and maintains validation procedures and criteria. The contractor shall provide adequate resources for performing validation processes, developing work products, and providing support services.

The Government or contractor shall validate the software to ensure it is suitable for use in its intended operating environment. Results from validation activity shall be analyzed and issues identified. Problems and nonconformances detected by the validation effort shall be documented and tracked to resolution ([3.1.10](#) and [3.3.3.8](#)).

When changes are made to a software system, either during initial development or during post release maintenance, sufficient contractor regression analysis and testing shall be conducted to demonstrate portions of the software not involved in the change were not adversely impacted. This is in addition to testing that evaluates the correctness of the implemented change(s). The specific validation effort necessary for each software change shall be determined by type of change, development products affected, and impact of those products on the operation of the software.

- a. The Government and contractor shall establish and maintain a validation plan. The contractor's validation plan shall be stored in IDE (3.1.5). The plan shall address:
 - 1) Resources, responsibilities, and schedule for validation task.
 - 2) Criteria for selecting items subject to validation or identification of items subject to validation.
 - 3) Validation tasks to be performed, including associated methods, techniques, and tools.
 - 4) Procedures for forwarding validation report/results to the cognizant MDA Program Office.
 - 5) Identification of validation work product and their appropriate configuration control.
 - 6) Method used to monitor and control the validation process against the plan.
 - 7) Review of activities, status, and results of the validation process with top-level management.
 - 8) Objective evaluation of validation processes against the process description, standards, and plans. This discussion shall address how noncompliances will be resolved.
- b. The Government and contractor shall establish and maintain a validation environment. The validation environment shall include, as appropriate:
 - 1) Requirements modeling tool.
 - 2) Test tools interfacing with the software being validated.
 - 3) Temporary embedded software.
 - 4) Recording tools for archiving and retrieving data for further analysis or replay.
 - 5) Models and simulations of subsystems, components, or interface systems.
 - 6) Real interface systems.
 - 7) Facilities and Government furnished software products or equipment.
 - 8) Trained and certified personnel (3.1.9) and subject matter experts.
 - 9) Test management tools, test case generators, test coverage analyzers, and emulators.
 - 10) Loads, stress, and performance assessment tools.

The contractor shall establish, maintain, and store in IDE (3.1.5) test requirements, test cases, and test specifications, which reflect their intended use.

3.3.3.4 Support of Independent Verification and Validation

The contractor shall support MDA IV&V efforts. This support includes:

- a. Providing work products and associated documentation.
- b. Participating in IV&V reviews of contractor's work products.
- c. Providing work areas for IV&V personnel.

- d. Access to development and test environments.

3.3.3.5 Independent Verification and Validation

The organization performing IV&V tasks and activities on MDA software products shall develop and implement an IV&V program IAW IEEE Standard 1012. A limited scope IV&V is required for Safety Critical Computing System Functions (SCCSF) per [3.14.7](#). The cognizant MDA Program Office shall select the IV&V organization.

3.3.3.6 Software Reviews

The Government and contractor shall hold periodic reviews assessing technical, performance, and schedule progress. Reviews shall assess the project's success in implementing software requirements of this provision. The contractor's software organization shall participate in or support all technical and mission assurance reviews ([3.4](#)), and safety working groups ([3.14](#)). A documented procedure shall be established and maintained to address participation in all software technical, management, and mission assurance reviews. Action items resulting from reviews shall be documented and tracked to resolution.

Program management shall review activities for managing software provisions IAW [3.1.2](#). This includes, but is not limited to, software development plans, project plans, test plans, process descriptions (e.g., standards, guides, and procedures), allocated requirements, software requirements, software design, software code, test plans, test procedures, and test cases.

Contractor's software engineering organization shall participate in review of products produced or acquired for or by other engineering groups (within the contractor's organization) to ensure products meet the receiving group's requirements and needs.

Results of software reviews shall be stored in IDE ([3.1.5](#)) by the contractor.

3.3.3.7 Software Audits

The contractor shall perform software audits IAW [3.1.8](#). Contractor software personnel performing reviews or audits shall be independent of personnel responsible for producing products or performing software activities. Software audits shall be held at predetermined milestones as specified in the SQA plan. Audit results shall be reported to software engineering management, software project management, and the contractor's top-level management, and stored in IDE ([3.1.5](#)).

Software audits shall ensure:

- a. Coded software products reflect design documentation, programming, and coding standards.
- b. Acceptance and testing requirements are adequate for acceptance of software products.
- c. Software products are successfully tested and meet their specifications.
- d. Test reports are correct and discrepancies between actual and expected results have been resolved.
- e. User documentation is complete, accurate, and meets specified standards.
- f. Activities have been conducted according to applicable requirements, processes, procedures, and plans.
- g. Cost and schedules adhere to established plans.

The contractor's software assurance program shall require software quality participation in preparation, review, and approval of software plans, standards, and procedures. Software quality shall review or audit

software engineering activities associated with software and firmware products to verify compliance with the SDP, procedures, and standards. Findings from reviews and audits shall be tracked to resolution ([3.1.8](#)).

3.3.3.8 Software Problem Reporting

The Government and contractor shall use the problem failure reporting and corrective action system ([3.1.10](#)) to report, investigate, analyze, and correct software nonconformances and problems. When problems, including nonconformances, have been detected in a software product or activity, a contractor's problem report shall be prepared and stored in IDE ([3.1.5](#)) to describe each problem. Resolutions and dispositions shall be reviewed to determine whether additional problems have been introduced. Requirements of this section supplement those of [3.1.10](#). Software nonconformance and corrective action reporting shall commence with baselining of a work product.

The contractor's software projects shall use defect prevention techniques to identify defect causes and provide assessment for potential process improvement opportunities ([3.3.1.5](#)). Responsibilities and authorities for implementing defect prevention activities shall be documented in software project plans.

The contractor's defect prevention program shall include causal analysis, periodic review and coordinated implementation of actions, documentation and tracking of defect prevention data, and feedback to software engineering and related groups on defect prevention activities.

3.3.3.9 Software Dependability

The contractor's software dependability program shall address:

- a. Identification and mitigation of risks associated with software failures.
- b. Emphasis on building in software error prevention, fault detection, isolation, recovery, and operating at reduced functional capability and degraded states.
- c. Measuring and analyzing defects in the software product during development to find and address problem areas within the software.

3.3.3.9.1 Software Reliability Program

The contractor shall establish and maintain a Software Reliability Program as an integral part of the overall Reliability Program, ensuring software reliability is a key focus area during system design and development enabling achievement of reliability requirements.

3.3.3.9.1.1 Software Reliability Program Plan

The contractor shall describe the planning and implementation of the Software Reliability Program in a Software Reliability Program Plan (SRPP). The contractor's SRPP may be integrated into the Reliability, Maintainability, and Availability Program Plan ([3.5.1](#)). The contractor shall ensure that methods to achieve, evaluate, and grow software reliability are distinctly identifiable. The plan shall describe the planning and implementation of software reliability activities. The contractor's SRPP shall address software specific management and technical tasks that are to take place within the overall reliability and software development programs, including techniques and methods for performing software reliability evaluation, and verifying that software products meet their allocated requirements. The SRPP shall define a process to ensure that appropriate methods and techniques are carried out at the correct point in development, including configuration control ([3.3.3.11](#) and [3.10](#)), and ensure adequate management of the project. The SRPP shall address the requirements contained within [3.3.3.9.1.1](#) through [3.3.3.9.1.6](#). If the SRPP is a standalone plan, then the SRPP shall be stored in IDE ([3.1.5](#)) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

The contractor's SRPP shall address:

- a. Software reliability requirements.
- b. Methods, techniques, and assumptions for allocating reliability requirements between hardware and software.
- c. Methods and assumptions used for deriving software reliability requirements from system software reliability requirements.
- d. Methods and techniques for software reliability achievement.
- e. Methods and techniques for measuring and verifying software reliability.
- f. Selection of software reliability models including identification and documentation of all limitations and assumptions.
- g. Procedures for software reliability progress reporting, including phasing of design reviews.

3.3.3.9.1.2 Software Reliability Documentation

The contractor's software reliability documentation shall be a readable overview of the evidence that the software meets its reliability requirements. The documentation shall include project development records and results of analyses and test of software components. The documentation shall be stored in IDE [\(3.1.5\)](#).

3.3.3.9.1.3 Allocation of Reliability Requirements to Software

The contractor shall allocate system reliability requirements to software configuration items. The contractor's Software Requirements Specification (SRS) shall include a statement of the numerical reliability goals for each identified software configuration item. The results of the software reliability allocation shall be incorporated into the system reliability modeling and prediction efforts defined in [3.5.5](#).

3.3.3.9.1.4 Software Reliability Analysis

The contractor shall perform software reliability analysis concurrently with design. The contractor shall use the following methods for requirements analysis for software reliability:

- a. Traceability Analysis. Each requirement in the software requirements, including derived requirements, shall be traced to the corresponding requirement in the Element Specification.
- b. Requirements inspections. The contractor shall carry out a formal inspection of software requirements.
- c. Failure Modes, Effects, and Criticality Analysis. Impacts of potential software failures shall be evaluated during Failure Modes, Effects, and Criticality Analysis (FMECA) [\(3.5.6.1\)](#).
- d. Checklists. The contractor shall develop checklists, based on data from previous projects, for reviewing the completeness and correctness of requirements.

Results of the Software Reliability Analyses shall be stored in IDE [\(3.1.5\)](#).

3.3.3.9.1.5 Software Reliability Evaluation and Achievement

The contractor shall define and implement a software engineering process that ensures the developed software will meet its reliability requirements. The contractor shall provide direct evidence of developing

software products reliability throughout the project. Direct evidence of software reliability shall come from testing, field data, fault data, and analyses.

The contractor shall carry out software reliability evaluation as part of normal system reliability tests and shall exercise the software in the system environment to demonstrate achievement of the software reliability requirements. The contractor shall use one or more of the following techniques or methods to perform software reliability evaluation:

- a. Reliability Growth Modeling. A technique shall be used to assess effectiveness of the software engineering process, and to predict when software will meet its reliability requirements.
- b. Statistical Testing. The demonstration of achieved software reliability through tests and trials. Tests can either be carried out with software installed in the system or a simulator.
- c. System Reliability Growth Testing. System reliability growth testing, as discussed in [3.5.10](#), provides reliability data under operational conditions.
- d. Performance Testing. Testing carried out to establish that non-functional performance requirements have been met.
- e. Analyses.

Results of the Software Reliability Evaluation shall be stored in IDE ([3.1.5](#)).

3.3.3.9.1.6 Fault Avoidance and Fault Tolerance

The contractor shall minimize software faults and control system failures due to any residual software faults. The contractor shall ensure that mission and safety critical software is dual fault tolerant which requires defensive programming (e.g., error detection, error handling, fail soft, and fail safe) and software diversity (i.e., use of two or more diverse programs to carry out critical functions).

3.3.3.10 Software Safety

The contractor's software safety program shall be performed IAW the safety provision [3.14](#).

3.3.3.11 Software and Firmware Configuration Management

The contractor's software and firmware configuration management activities shall be performed IAW provision [3.10](#) and the following requirements. The requirements of this section also apply to software and firmware items that are supplied as GFI, GFE, COTS, and NDI. Software and firmware products to be placed under Configuration Management (CM) control shall be identified in the CM plan along with the milestone associated with placing the product under control. Each project software and firmware library system used as a repository for software and firmware baselines shall be documented in the CM plan.

3.3.3.11.1 Software Configuration Items

For each SCI, the contractor shall identify its corresponding Software Components (SC) and Software Units (SU). For each SCI, SC, and SU the contractor shall issue or obtain a software identifier, which consists of a name or number and a version identifier, and relates the software to its associated software design documentation, revision, and release date ([3.10.3.3.1](#)). The contractor shall embed the software and version identifiers within the source code, and provide a method for display of the software and version identifier data to the user upon command. The marking and labeling of software media shall include a software identifier and version.

3.3.3.11.2 Software and Firmware Change Control Process

The contractor's change control process ([3.10.4](#)) shall address how software and firmware changes are to be identified, documented, submitted, reviewed, approved or disapproved, implemented, verified, and released. The contractor's Configuration Control Board shall have appropriate disciplines represented to process software and firmware changes.

The contractor's change control process shall ensure only authorized changes are implemented into software and firmware products. The configuration control system shall ensure any referenced version of software and firmware can be regenerated from backups.

The configuration control process shall address controls over, and changes to, tools used in code generation and testing of deliverable software and firmware product. It shall also address how legacy software and firmware and other supplied (e.g., GFE, GFI, NDI, or third party) software and firmware (e.g., source, executable, or data) shall be protected against corruption.

The configuration control process shall address variances (waivers and deviations) ([3.10.4.6](#)) associated with software and firmware activities and products. Variances shall be documented, reviewed, and resolved with the appropriate software and firmware engineering manager, project manager, and other appropriate groups.

3.3.3.11.3 Software Library

The contractor shall establish and maintain a software library system to facilitate control of software products. Software library systems shall provide a method for storage of current and superseded versions of software programs, and software tools required to maintain and use software. The library system shall provide for:

- a. Maintenance of and controlled access to approved configurations of software programs and associated design disclosure documentation.
- b. Maintenance of software tools and related documentation.
- c. Controls to assure integrity of software programs and associated documentation.

The contractor shall implement a process governing how software products are created, entered, updated, and released from the software library. This process shall address controls imposed over software products throughout their life.

The contractor shall maintain a second off site repository containing duplicate files of all software programs including both source and executable versions of all software, build scripts and their corresponding SVD for each version, design disclosure documentation, and support software or tools to allow for retrieval in the event of a disaster.

The contractor shall verify and certify to the cognizant MDA Program Office that software libraries contain no trapdoors, back doors, or malicious code.

The contractor shall ensure all status indications from library routines are processed. Error status indications shall not be ignored.

3.3.3.11.4 Software Configuration Audits

The contractor shall perform a software baseline configuration audit to determine completeness, accuracy, consistency, and quality before establishment of software baselines (e.g., allocated, requirements, architecture, and design). Software configuration change audits shall be conducted to ensure that only approved changes are incorporated into the software product or its technical descriptions. The contractor shall support software functional and physical configuration audits IAW

[3.10.6](#). The contractor shall perform in process SCM audits to be conducted throughout the life cycle to determine compliance with SCM policies, plans, standards, processes, and procedures. Results of SCM audits and finding resolutions shall be stored in IDE ([3.1.5](#)).

Problems identified as a result of audits shall be documented, tracked, controlled, and resolved.

3.3.3.11.5 Software Status Accounting

The contractor's status accounting system ([3.10.5](#)) shall provide management with records and reports to show status and history of controlled items. Status reports shall include status of proposed and approved changes for each SCI, SC, and SU, outstanding variances (waivers and deviations), outstanding problem reports, latest software item versions, release identifiers, number of releases, and comparisons of releases. Status accounting system shall provide a correlation between configuration status of the software program, its documentation, and associated hardware. Configuration management status reports shall be developed and stored in IDE ([3.1.5](#)). The contractor's software configuration status accounting file shall be available and current for each project milestone.

3.3.3.11.6 Software and Firmware Media Generation

The contractor shall establish and maintain a controlled system to assure integrity of deliverable software, firmware, and data before and after transfer to transportable media, nonvolatile memory, deliverable hardware, or test and inspection equipment. This system shall include verification that each copy of software or data is an accurate replication of the master copy retained in the library. Results of these media generation and verifications shall be documented and maintained as quality records, and stored in IDE ([3.1.5](#)).

3.3.3.12 Software Documentation

The contractor shall establish and maintain a documentation process for recording information produced by a software task, activity, or process. Process documentation shall define the set of activities which plan, design, develop, produce, edit, distribute, and maintain those documents needed by managers, engineers, and users of the system or software product. Process or project documentation shall be updated to reflect improvements.

The contractor's software process documentation shall include:

- a. Software models, tools, and techniques approved for use.
- b. Guidelines and criteria for tailoring the organization's standard software processes.
- c. Requirements and guidelines for establishing and maintaining software process databases.
- d. A library and guidelines for software process related documentation (e.g., procedures, manuals, project plans, and standards).

Configuration management controls shall govern software documentation. The Government and contractor shall verify software documentation is available, adequate, current, complete, and consistent.

3.3.4 Firmware Development Plan

The contractor shall provide a plan addressing the development process for digital electronics (e.g., integrated circuits, memory devices, or programmable logic devices). The plan shall describe:

- a. The organizations involved with development of digital electronics, their responsibilities, and interrelationships.
- b. The devices to be incorporated into the design and their pedigree.

- c. The process for configuration management of firmware IAW [3.10](#).
 - 1) Firmware version shall be identified on the component, drawings, and process documentation.
 - 2) The contractor shall certify gate logic and any software or data resident on a firmware device is consistent with labeling of the component.
- d. Any required development tools or languages (to include standards).
- e. The design verification process including plans for peer reviews of Hardware Description Language files, schematics, macro generators, and software tools. This includes addressing how firmware functionality will be verified when hosted on physical components.
- f. The process for implementing the design as a physical device.
- g. The planned testing and evaluation of the digital electronic device or circuit.
- h. The process for incorporating the electronic device into the overall system.

The contractor's Firmware Development Plan and all updates shall be submitted into IDE ([3.1.5](#)) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. The Firmware Development Plan shall be maintained consistent with current project requirements. The contractor shall maintain records of all firmware planning, re-planning efforts, and test results and shall make these available to the cognizant MDA Program Office via the IDE ([3.1.5](#)).

3.4 Technical and Mission Assurance Reviews

The contractor shall support Government technical and mission assurance reviews to ensure the design meets mission requirements and to reduce mission risk to acceptable levels. Reviews shall be tailored to specific needs of each program and mission based on risk, schedule, and funding. Results from these reviews shall be documented and action items tracked to resolution.

3.4.1 Technical Reviews

The contractor shall support Government technical reviews to determine design maturity and to ensure the design is technically adequate and meets requirements. Technical reviews shall be event driven and conducted at appropriate points in development when progress merits review to check design maturity, review technical risk, and determine whether to proceed to the next level of development. Technical reviews shall be integrated into the systems engineering process and conducted by a joint Integrated Product Team (IPT) composed of MDA representatives and contractor personnel and attended by non-advocate technical personnel. Formal technical reviews shall be preceded by a series of technical interchange meetings where issues, risks, problems, and concerns are surfaced and addressed. The technical review will be used as a confirmation of completed effort, not a forum for problem solving. In preparation for technical reviews, the contractor shall make available to review participants via IDE (3.1.5), necessary documentation, material, and analyses regarding the design in advance of the scheduled event to allow sufficient time to examine the information in detail. Information such as specifications, results from tradeoff studies and design analyses, drawings, manuals, schedules, design and test data, risk analyses and mitigation activities, interface specifications, test methods and plans, code, technical plans, and metrics may be needed for review. Technical reviews may be conducted at both contractor and supplier sites. For each review the contractor shall:

- a. Provide necessary agenda, plans, administrative support, and facilities.
- b. Ensure participation by subject matter experts including suppliers.
- c. Provide information and items necessary to demonstrate and confirm that accomplishments associated with the specific review event are satisfied.
- d. Substantiate trade-off decisions with technical details and associated rationale.
- e. Document proceedings with associated rationale for key points, decisions, and issues.
- f. Document all open and unresolved items with their closure requirements and due dates, and assign organizations responsibilities.
- g. Identify risks, including safety risks (3.1.6).

Technical reviews shall be tailored to specific program needs. The following set of reviews depicts a normal sequence in terms of assessing technical progress from concept through production. The contractor shall participate in the following reviews as directed by the cognizant MDA Program Office. Additional reviews may be required on a program-by-program basis. Entrance and exit criteria for MDA Technical Reviews are documented in Appendix A of the Ballistic Missile Defense System (BMDS) Systems Engineering Plan (SEP), and supplemented in the following paragraphs. Throughout this document the BMDS SEP will be abbreviated as the BMDS SEP.

Results of Technical Reviews and any associated actions shall be stored in IDE (3.1.5).

3.4.1.1 Initial Technical Review

The Initial Technical Review (ITR) assesses the capability needs and materiel solution approach of a proposed program and verifies that the requisite research, development, test and evaluation, engineering, logistics, cost, and BMD System Description Document reflects the complete spectrum of technical

challenges and risks. The contractor shall present objective evidence verifying completion of entrance and exit criteria specified in the BMDS SEP.

3.4.1.2 Alternative Systems Review

The Alternative Systems Review (ASR) assesses the preliminary materiel solutions evaluated during the Materiel Solution Analysis phase. The ASR ensures that one or more proposed materiel solutions has the best potential to be cost effective, affordable, operationally effective and suitable, and can be developed to provide a timely solution to a need at an acceptable level of risk. The contractor shall present objective evidence verifying completion of entrance and exit criteria specified in the BMDS SEP.

3.4.1.3 Systems Requirements Review

The Systems Requirements Review (SRR) is a multi-disciplined technical review to ensure that the system under review can proceed into initial systems design, and that all system requirements and performance requirements derived from the Initial Capabilities Document or draft Capability Development Document are defined and testable, and are consistent with cost, schedule, risk, technology readiness, and other system constraints. The contractor shall present objective evidence verifying completion of entrance and exit criteria specified in the BMDS SEP. In addition to criteria identified in the BMDS SEP, the contractor shall present objective evidence verifying Quality, Safety, and Mission Assurance requirements are identified and incorporated into program planning.

3.4.1.4 System Functional Review

The System Functional Review (SFR) is a multi-disciplined technical review to ensure that the system's functional baseline is established and has a reasonable expectation of satisfying the requirements of the Initial Capabilities Document or draft Capability Development Document within the currently allocated budget and schedule. The contractor shall present objective evidence verifying completion of entrance and exit criteria specified in the BMDS SEP. In addition to criteria identified in the BMDS SEP, the contractor shall present objective evidence verifying the Capability Development Document is approved by the Government (i.e., entrance criterion) and the implementation requirements for technology transition are defined (i.e., exit criterion).

3.4.1.5 Software Specification Review

A Software Specification Review (SSR) ensures the Software Configuration Item (SCI) requirements as specified in the Software Requirements Specification (SRS) and the Interface Requirements Specification (IRS) are sufficiently mature to initiate preliminary design efforts. The contractor shall present objective evidence verifying the completion of the following entrance and exit criteria:

Entrance Criteria:

- a. No outstanding action items.
- b. Documentation is complete for software requirements, software processes, and tools. If an incremental approach is used, the documentation must be complete for the increment.
 - 1) Software Requirements Specification and external IRS for the SCI completed and distributed for review and comment.
 - 2) Software development tools for establishment and maintenance of software development environment are in place and operational.
 - 3) Baseline higher level system and subsystem design specifications accepted.
- c. Software metrics collected and analyzed.

- d. Software related item performance specifications validated.
- e. Software Configuration Item requirements traced to higher level (subsystem and system) requirements.
- f. Cost, schedule, and performance risks identified, quantified, and prioritized.
- g. Systems Engineering:
 - 1) Common operational environment performance analysis performed.
 - 2) Functional Architecture reviewed for System Safety Critical Functions.
- h. Software Quality requirements established (i.e., correctness, reliability, efficiency, integrity, usability, maintainability, testability, flexibility, portability, reusability, and interoperability) including those relating to the SRSs and IRSs.
- i. Testing:
 - 1) Agreement on qualification requirements identifying applicable levels and methods of testing for the software requirements.
 - 2) Test resources, infrastructure, and costs identified for various levels of testing.

Exit Criteria:

- a. Software Requirements Specification and the IRS trace to and fully implement the system level requirements allocated to software.
- b. Software requirements (including software interface requirements), based on the selected software life cycle model, specified to the level of completeness called for in the Software Development Plan (SDP).
- c. Software requirements include necessary requirements derived from system and software architecture, system operational concepts, trade studies, or design decisions.
- d. Non-Developmental Items (NDI) fully integrated into components of the software architecture.
- e. The SDP is consistent with the Integrated Master Plan, and Systems Engineering Management Plan.
- f. The SDP addresses the full software development life cycle.
- g. Computer hardware and software compatibility evaluated.
- h. Human interfaces, controls, and displays evaluated.
- i. Software related risks identified, properly documented, and mitigation plans established.
- j. All designs consistent with System Operational Concepts.
- k. Safety risks addressed.

3.4.1.6 Preliminary Design Assessments/Critical Design Assessments

The contractor shall perform Preliminary Design Assessments (PDA) and Critical Design Assessments (CDA) with participation by the cognizant MDA Program Office or designated technical representative(s).

The PDAs are focused, in-depth working-level technical design reviews, conducted incrementally, that support the evolving design and development of a product and occur before a Preliminary Design Review (PDR). The CDAs are focused, in-depth working-level technical design reviews, conducted incrementally, that support the detailed design development of a product and occur before Critical Design Review (CDR). Both assessments address specific functional areas or aspects of a design to demonstrate requirement satisfaction. These assessments are an outgrowth of technical working groups and follow the format and guidelines described for PDR and CDR. Data generated in preparation for, and as a result of, these reviews will support preparations for PDR and CDR. These are working-level meetings and can represent a dry run of PDR and CDR presentation material. Independent technical experts (representative(s) not assigned to the project) ensure all requirements are met, the design approach is verified, risks are identified, and mitigation plans are generated.

3.4.1.7 Preliminary Design Review

Preliminary Design Reviews (PDR) are conducted by the cognizant MDA Program Office before the detail design process to evaluate progress and technical adequacy of the selected design approach, determine its compatibility with performance requirements of the specification, and establish the existence and physical and functional interfaces between the item and other items of equipment or facilities. A series of PDRs are normally held for each Configuration Item (CI) or aggregate of CIs, or subsystem, leading to a system PDR for completion. The contractor shall present objective evidence verifying completion of entrance and exit criteria specified in the BMDS SEP. In addition to criteria identified in the BMDS SEP, the contractor shall present objective evidence verifying completion of the following exit criteria.

Exit Criteria:

- a. Software functionality in the approved allocated baseline is consistent with updated software metrics and resource loaded schedule.
- b. Reliability, maintainability, testability, availability, producibility, and supportability analyses indicate conformance to approved system or subsystem specifications.
- c. Technical Performance Measurement data and analysis indicate the end item will satisfy performance requirements.
- d. Risks associated with safety hazards can be mitigated to an acceptable risk level within the existing budget.
- e. Program Quality, Safety, and Mission Assurance requirements identified and incorporated into procedures and verified.
- f. Verification plans approved and resources available to continue to CDR.

3.4.1.8 Critical Design Review

Critical Design Reviews (CDR) are conducted when detail designs are essentially complete, configuration documentation is ready for release, and the configuration item is ready for fabrication or coding. The CDRs are conducted to determine that detail designs satisfy design requirements established in the specification and establish the interface relationships. The contractor shall present objective evidence verifying completion of entrance and exit criteria specified in the BMDS SEP. In addition to criteria identified in the BMDS SEP, the contractor shall present objective evidence verifying completion of the following exit criteria.

Exit Criteria:

- a. Safety and mission critical items identified.

- b. Schedules for completion of software development consistent with status of software design at the time of CDR.
- c. Key product characteristics impacting system performance, assembly, cost, reliability, or safety identified.
- d. Critical manufacturing processes that impact key characteristics identified and their capability to meet design tolerances determined.
- e. Process control plans developed for critical manufacturing processes.
- f. Program Quality, Safety, and Mission Assurance requirements implemented at contractors, subcontractors, and suppliers.

3.4.1.9 Test Readiness Review

Test Readiness Reviews (TRR) are conducted for each critical subsystem to confirm completeness of test procedures, to ensure subsystem/system is ready for testing, and to ensure the performing activity is prepared for formal testing. The TRR shall be conducted after the critical gate process (3.7.7.2) is completed. The contractor shall present objective evidence verifying completion of entrance and exit criteria specified in the BMDS SEP. In addition to criteria identified in the BMDS SEP, the contractor shall present objective evidence verifying completion of the following entrance and exit criteria:

Entrance Criteria:

- a. No outstanding action items.
- b. The testing objectives clearly defined and documented. Test items, plans, procedures, environments, and configuration support those objectives.
- c. Configuration of the system under test approved. All interfaces under configuration control.
- d. All applicable functional and qualification testing conducted successfully.
- e. All TRR specific materials (e.g., test plans, test cases, and procedures) available to all participants prior to conducting the review.
- f. All known system discrepancies identified and dispositioned in accordance with an approved plan.
- g. All previous design review success criteria and key issues satisfied in accordance with an approved plan.
- h. All required test resources (e.g., personnel, facilities, test articles, and test instrumentation) identified and available to support required tests.
- i. Roles and responsibilities of all test participants defined and approved.
- j. Test contingency planning accomplished and all personnel trained.

Exit Criteria:

- a. Test procedures comply with test plans and descriptions, demonstrate adequacy to accomplish test requirements, and satisfy subsystem specification requirements for verifications.
- b. Test plans for the system under test completed and approved.

- c. Test requirements planned to be verified at this test event are approved.
- d. Bi-directional traceability is provided between requirements under test and test cases, and test procedures in which requirements will be verified.
- e. The end item (i.e., hardware, software, and firmware) is under configuration control.
- f. Test environment, including hardware, software, and firmware, is validated.
- g. Government and contractor personnel roles and responsibilities well defined.
- h. Previous test results (e.g., dry runs, pre-mission tests, and runs for record) demonstrate safety and mission critical items meet the test objectives.
- i. Required operation and support documents are complete and accurate.
- j. Data acquisition, handling, and analysis provisions prepared and approved.
- k. All moderate and high risks acceptable to MDA.

3.4.1.9.1 MDA Executive Level Test Reviews

The Government and contractor shall support MDA executive level test reviews as defined in MDA Directive 3200.03. Specific direction on test event phase reviews and executive reviews is provided in Ballistic Missile Defense System Test Concept of Operations document. The MDA executive level test review process provides the structure needed to assure MDA senior leadership that critical issues involved in planning, preparation, and execution of a test are satisfactorily resolved before the test event and test results yielded the desired data and analysis. Each test review briefing is intended to provide proof for MDA senior leadership to authorize proceeding with next test phase. These guidelines apply to all MDA elements and system level tests. This process can be tailored per MDA Directive 3200.03.

3.4.1.10 System Verification Review

System Verification Reviews (SVR) assess system functionality and determine if the system satisfies functional requirements (derived from the Capability Development Document and Capability Production Document) documented in the functional baseline. The SVR outcome verifies final product performance, provides inputs to the Capability Production Document, and ensures the system can proceed into Initial Production. The SVR is often conducted concurrently with the Production Readiness Review. The contractor shall present objective evidence verifying completion of entrance and exit criteria specified in the BMDS SEP. In addition to criteria identified in the BMDS SEP, the contractor shall present objective evidence verifying completion of the following exit criteria.

Exit Criteria:

- a. Test and analysis results verify that the system is both operationally effective and suitable for its intended use.
- b. Safety assessment completed.

3.4.1.11 Functional Configuration Audit

A Functional Configuration Audit (FCA) shall be conducted by the contractor with Government participation for each CI and by the Government with contractor participation for the overall system. The FCA may occur concurrently with the SVR and Production Readiness Reviews (PRR). The contractor shall examine the as-tested characteristics of a CI (hardware and software) with the objective of verifying that actual performance complies with design and interface requirements in the functional baseline. The contractor shall review the configuration item's test and analysis data, including modeling and simulation,

and software unit test results to verify the intended function or performance stated in its specification is met. For large systems, FCAs may be conducted on lower level CIs for specific functional areas and may address non-adjudicated discrepancies as part of the FCA for the entire system.

A successful FCA typically demonstrates the Product Development Phase product is sufficiently mature for entrance into Initial Production.

The Government and contractor may use MIL-HDBK-61A paragraphs 8.2.2.1 and 8.3 as additional guidance for conducting a FCA.

3.4.1.12 Production Readiness Review

Production Readiness Reviews (PRR) are conducted in an iterative fashion, concurrently with other technical reviews (e.g., SVR and PCA), during Product Development Phase. The PRR shall be performed by the Government and contractor for each CI, system, subsystem, and safety and mission critical item to determine if the design is ready for production and if the prime contractor and major subcontractors have accomplished adequate production planning with acceptable risks including thresholds of cost, schedule, performance, or other established criteria.

Each CI, system, subsystem, and safety and mission critical item shall be evaluated to determine that it correctly and completely implements all system requirements, and whether traceability of final system requirements to the final production system is maintained. The cognizant MDA Program Office shall designate an IPT to assess the state of readiness of manufacturing processes, the Quality System, production planning (i.e., facilities, tooling, and test equipment capacity), personnel development and certification, process documentation, inventory management, and supplier management; and identify production risks to MDA.

The final PRR should occur at completion of the Product Development Phase and the start of the Production Phase. The final PRR should assess manufacturing and quality risk as the program proceeds into Initial Production.

The cognizant MDA Program Office or designated IPT should tailor length and depth of a PRR based on technical maturity and complexity of the configuration item, system, subsystem, or safety and mission critical item being evaluated.

The contractor shall present objective evidence verifying completion of the following entrance and exit criteria.

Entrance Criteria:

- a. No outstanding action items.
- b. The significant production engineering problems encountered during development are resolved.
- c. Design documentation adequate to support production.
- d. Production plans and preparation adequate to begin fabrication.
- e. Production enabling products and adequate resources available, allocated, and ready to support end product production.

Exit Criteria:

- a. System product baseline established and documented to enable hardware fabrication and software coding to proceed with proper configuration management.

- b. Capability Production Document finalized and approved.
- c. Adequate processes and metrics established.
- d. Technical, programmatic, and cost risks identified, properly documented, and manageable ([3.1.6](#)).
- e. Program schedule executable within anticipated cost and technical risks.
- f. Program staffed properly.
- g. Technologies sufficiently mature for production.
- h. Detailed design producible within the production budget.
- i. Production facilities ready and personnel trained.
- j. Detail design complete and stable enough to enter Initial Production.
- k. Process Failure Modes and Effects Analysis ([3.5.14](#) and [3.12.6.1](#)) is performed before start of production for ordnance, safety and mission critical items, and potential process failure modes identified with actions taken to mitigate risk.
- l. Supply chain established and stable with materials available to meet planned Initial Production.
- m. Manufacturing processes demonstrated and proven in a production representative environment with at least an Engineering Manufacturing Readiness Level of 4 and Manufacturing Readiness Level of 8 ([3.2.18.1](#)).
- n. Producibility trade studies and risk assessments completed.
- o. Validated production cost model based upon stable detailed design.
- p. Environmental Safety and Occupational Health residual risks identified and manageable.

3.4.1.12.1 Follow On Production Readiness Review

A follow on tailored PRR shall be performed by the Government and contractor in the Production phase if:

- a. Changes occur in the design, materials, or manufacturing processes after PRR.
- b. Production startup or restart occurs after a 12 month shutdown period.
- c. Production startup occurs with a new contractor.
- d. Manufacturing site relocation occurs.

3.4.1.13 Physical Configuration Audit

A Physical Configuration Audit (PCA) shall be conducted around the time of the Production Decision, or as soon as production representable systems are available. The PCA is normally conducted if the cognizant MDA Program Office plans to control detail design of the item it is acquiring via a Technical Data Package. If the cognizant MDA Program Office does not plan to exercise such control or purchase the item's Technical Data Package, the contractor shall conduct an internal PCA to define the starting point for controlling the CIs detail design and establishing a product baseline.

The PCA shall examine the as-built configuration of a CI against its design documentation. The PCA shall ensure acceptance testing requirements prescribed by the documentation are adequate for acceptance of production units. The PCA shall include a detailed audit of engineering drawings, specifications, technical data, tests used in production of CIs and design documentation, listings, and operation and support documents for SCIs. The PCA shall include audit of released engineering documentation and quality control records to ensure the as-built or as-coded configuration is reflected by this documentation. For software and firmware, the product specification, Interface Design Document, and Version Description Document shall be part of the PCA.

Satisfactory completion of a PCA and approval of the product specification are necessary for the cognizant MDA Program Office to establish the production baseline for a CI.

The Government and contractor may use MIL-HDBK-61A paragraphs 8.2.2.2 and 8.3 as additional guidance for conducting a PCA.

3.4.2 Mission Assurance Reviews

Mission Assurance Reviews shall be performed by the Government with contractor participation to clarify and ratify mission requirements (i.e., planning and design), discuss issues and approaches, and communicate decisions. Reviews ensure known issues and problems are dispositioned before each critical event. The cognizant MDA Program Office shall provide technical experts as panel members. Completion of activities necessary to fulfill specific readiness review criteria shall also be accomplished during Mission Assurance Reviews. The contractor shall participate in Mission Assurance Reviews as required. The following sections describe Mission Assurance Reviews, which are used as a sequential process to mitigate risk and assure mission success. The Government and contractor may propose a Mission Assurance Review process tailored for a particular system as an alternate to the process described below. The results of Mission Assurance Reviews shall be recorded by the contractor and stored in IDE [\(3.1.5\)](#).

Mission Assurance Reviews do not replace other Government reviews or certifications required by contract, federal regulation, or law.

3.4.2.1 Mission Readiness Review

The contractor shall support and participate in a Mission Readiness Review conducted 4-6 weeks before launch. The review shall address all components of mission readiness: project status, test objectives and mission performance, instrument readiness, launch vehicle readiness, ground system readiness, launch service readiness and launch site assessment, resolution of all open items, liens and waivers, public affairs plan, safety assessment, and other topics, to ensure all aspects critical to mission success have been reviewed. The Mission Readiness Review results shall be presented to the mission review board for review and certification of the readiness of all mission components to proceed toward launch.

3.4.2.2 Pre-Environmental Review

Before start of acceptance testing, the contractor shall participate and support a Pre-Environmental Review (PER) to assess readiness of flight hardware, software, and required environmental test facilities. The PER shall occur before the start of environmental testing of the prototype or flight system. The primary purpose of this review is to establish readiness of the system for test and evaluate environmental test plans. The PER shall be held before full system integration and functional test in preparation for environmental testing.

3.4.2.3 Pre-Shipment Review

The contractor shall support the Pre-Shipment Review (PSR). The review shall be conducted before shipment of flight test assets for integration with ground support system or launcher at a test range. This review shall address hardware build up, acceptance test results, and pedigree data [\(3.1.7\)](#). Hardware on times or cycle times shall also be reviewed and shown to be within acceptable limits. The contractor shall

provide status of safety items, deliverable documents, and any subsequent launch range issues or necessary approvals before sending flight hardware to a range. The contractor and Government representative(s) will assess data and provide a recommendation of whether to ship hardware and software. Additionally, the contractor shall be prepared to present and discuss objective evidence verifying completion of the following exit criteria:

- a. An end item data package is compiled which reflects the As-Built versus As-Designed configuration. The end item data package is reviewed and all outstanding action items dispositioned.
- b. Analysis of interfaces between units (inter/intra-subsystem, inter-segment, and inter-system) completed.
- c. User guides and operations manuals are revised incorporating the final testing lessons learned before shipment.
- d. Hazards identification and analysis of system hardware and software, the system environment, and its intended use are completed.
- e. Mishap risk assessments are completed to define severity and probability of each identified hazard on personnel, facilities, equipment, operations, the public, the environment, and the system itself.
- f. Compliance with ground operations safety requirements verified.
- g. Equipment (including test equipment, tooling, and Ground Support Equipment) that will be used at the launch site is certified, calibrated, and proof loaded prior to shipment and is compliant with Range Safety requirements.
- h. A packaging, handling, storage, and transportation plan completed before shipment.
- i. Customer-owned and Government Furnished Equipment identified prior to shipment.
- j. Program risks are identified and mitigation acceptable to the cognizant MDA Program Office, MDA/DE, and MDA/QS.
- k. The cognizant MDA Program Office and MDA/QS concurrence obtained that all controls are in place for shipment.

3.4.2.4 Mission Operations Review

The contractors shall participate and support a Mission Operations Review (MOR) before significant integration and test of flight systems and ground data systems. The MOR establishes status of the system components, including the ground data systems and their operational interface with flight systems. Discussions shall include mission integration, test planning, safety assessment, and status of preparations for flight operations.

3.4.2.5 Flight Operations Review

The contractor shall participate and support a Flight Operations Review (FOR) to assess adequacy of final operation plans and compatibility of flight components with ground support equipment and ground network, including results of network compatibility tests. The FOR is held after the system is configured for launch. The purpose of the FOR is to: (1) examine demonstrations, tests, analyses, and audits, which determine system readiness for safe and successful launch and subsequent flight operations; and (2) ensure all flight and ground hardware, software, personnel, and procedures are ready and compatible.

3.4.2.6 Pre-Flight Readiness Review

Before the decision to conduct a flight test, the contractor shall support a Pre-Flight Readiness Review,

during which a Government panel will conduct a detailed review of the readiness of the flight test design, test asset, target, and test range for conduct of the mission. Developmental and system readiness testing for all test unit components and associated support sub-elements shall be reviewed, including results from any flight test unit problems or anomaly investigations, associated resolutions, and documentation (including a summary of the Pre-Shipment Review conclusions). As part of this review process, the contractor shall provide results from qualification testing to demonstrate all critical components are fully qualified for expected flight conditions, including margins (at least 3 dB above predicted environments) to handle unexpected conditions. Target test and pedigree data will be reviewed. Ground system acceptance testing and integrated testing of ground support systems shall be reviewed along with data for all system interfaces. Additionally, range countdown and launch procedures and processes will be reviewed. Flight safety analyses (addressing destruct limit lines and debris patterns) shall be confirmed as acceptable. This process shall also include certification of the flight test scenario and associated flight objectives. Accredited modeling and simulation results (including hardware-in-the-loop test data) shall be used to provide flight test performance predictions and demonstrate that all flight test objectives will be met. This overall process shall culminate in a series of meetings conducted to obtain MDA Director approval to perform the flight mission.

3.4.2.7 Launch Readiness Review

The contractor shall participate and support a Launch Readiness Review (LRR) to assess overall readiness of the total system to support mission flight objectives. The LRR shall be held at the launch site not less than two to three days before launch. The review shall cover all activity since PSR, closure of any required actions, and summation of all testing and launch operations planning and rehearsals to the present. Any residual risks, including safety, shall be presented at this time. Closure of this review and any actions generated from the review indicate the mission is ready for launch.

3.5 Reliability, Maintainability, and Availability

The Government and contractor shall establish and maintain a Reliability, Maintainability, and Availability (RM&A) program as an integral part of system design and development process to track the design's ability to meet or exceed the product's mission requirements. The program shall provide tools used to create designs at reduced total ownership cost and identify problem areas in design that require additional development. An effective RM&A program executed during design and development will improve BMDS and element level operational readiness and mission success, reduce item demand for maintenance and logistic support, and provide essential risk management information.

3.5.1 Reliability, Maintainability, and Availability Program Plan

The Government and contractor shall develop and maintain a RM&A Program Plan that describes planning and implementation of RM&A activities including tests, analyses, and associated ground rules and assumptions. Additionally, the plan shall include specific reliability design criteria that define both appropriate and inappropriate devices, materials and processes for the design's application based historical data, and new technology assessments. The contractor's RM&A Program Plan shall be submitted into IDE ([3.1.5](#)) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.5.1.1 Reliability, Maintainability, and Availability Program Planning

The contractor's RM&A Program planning shall identify RM&A tasks to be performed, and describe how RM&A tasks will be implemented and controlled. Planning shall identify scheduling of RM&A tasks relative to project events. The planning effort shall identify activities that ensure RM&A functions are an integral part of design and development processes and that RM&A functions interact effectively with other project disciplines, including systems engineering, hardware, software, logistics, safety, design, and mission assurance. The planning effort shall also identify how reliability assessments will be integrated with the design process and other assurance practices to maximize probability of meeting mission success criteria.

3.5.2 Supplier Reliability, Maintainability, and Availability Requirements

The contractor shall establish and maintain management procedures and design controls, including allocation and flow down of RM&A requirements to safety and mission critical suppliers. Plans and data to support specified RM&A requirements shall be stored in IDE ([3.1.5](#)).

3.5.3 Failure Reporting, Analysis, and Corrective Action System

As part of the overall closed loop problem and failure reporting and corrective action system ([3.1.10](#)), the Government and contractor shall establish and maintain a closed loop Failure Reporting, Analysis, and Corrective Action System (FRACAS). The FRACAS shall provide a management tool to identify, correct, and prevent further recurrence of hardware, software, and firmware failures during system development, fabrication, testing, and operations. The FRACAS shall ensure failures, from first incidence, are documented, analyzed and timely corrective actions are taken to prevent recurrence.

The BMDS Failure Review and Corrective Action System, acting under the Single Technical Authority, shall disposition and track closure of BMDS anomalies that adversely affect BMD system performance. Sources of BMDS anomalies may include test events, operational concerns, Operational Test Agency issues, or issues nominated by the engineering community or MDA Leadership. The Government will use the MDA Failure Review, Analysis, and Corrective Action System Charter and Instruction for implementing the BMDS Failure Review, Analysis, and Corrective Action System.

The contractor's closed loop feature of FRACAS requires information obtained during failure analysis be disseminated via IDE (3.1.5) for information and further action, if necessary, to all decision making program engineers, managers, the cognizant MDA Program Office or designated representative(s). The contractor may use MIL-HDBK-2155 as additional guidance for implementing a FRACAS.

3.5.4 Failure Review Board

The Government and contractor shall establish a process to convene a Failure Review Board (FRB) to review failures to safety and mission critical items. Failures that preclude accomplishment of written primary objectives or have significant impact to BMDS performance, and occur while preparing for or during MDA Element or BMDS level events, including demonstrations, tests, exercises, and operations, shall undergo a formal failure review process conducted by a MDA appointed FRB IAW MDA Directive 6055.05. Accident and mishap safety investigations shall be conducted IAW MDA Instruction 6055.02-INS. Failures that occur during manufacturing and factory testing shall be reviewed by the contractor. Contractor FRB members shall include the cognizant MDA Program Office, or designated representative(s), and, as appropriate, representatives from reliability, design, manufacturing, quality, and system safety. The failure review process shall include assessment of failures, failure data documented in FRACAS, failure trends, and corrective action status and effectiveness. The FRB shall examine failure data, including a description of test conditions at the time of failure, symptoms of failure, failure isolation procedures, and known or suspected causes of failure. Open FRB items shall be tracked until root cause failure mechanisms have been satisfactorily identified and corrective action initiated and verified. The FRB objective shall be to improve reliability and maintainability of hardware and associated software. All failure occurrence information shall be available to the Government and contractor FRBs. A break-of-configuration is not allowed without prior FRB approval. All failures shall require closeout approval by the FRB.

3.5.4.1 Unverified Failures

The Government and contractor shall establish and maintain a process addressing how hardware, software, and firmware unverified failures shall be processed for safety and mission critical items. As a minimum, the unverified failure process shall address the failure review board process, criteria to declare a failure as unverified, an engineering risk assessment, and the risk acceptance authority. The contractor's process shall be documented and submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office and MDA/QS. Notification that this documented process is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.5.5 Reliability Modeling, Allocation, and Prediction

The Government and contractor shall develop and maintain a reliability model (reliability block diagrams and math models) for each system, subsystem, and lower levels with associated allocations and predictions for all items (i.e., hardware and software) in each reliability block. Each block shall include function and item identification to a level consistent with design maturity. Basic reliability and mission reliability requirements shall be used to establish baseline requirements for designers.

Reliability allocation shall be based on mission and configuration item reliability requirements. Reliability requirements shall be allocated to each indenture level (i.e., hardware and software) and, as applicable, imposed on suppliers.

Reliability predictions shall be derived and applied down to the level of individual piece parts and software units. The Government and contractor shall update reliability predictions as the design matures and valid test data become available. Results of reliability predictions shall be used as inputs in formulating decisions for product design, safety, maintenance, logistics, and availability analyses. Failure rate data used in predictions shall be selected from sources that reflect the intended application. Predictions for electrical, mechanical, structural, optical, and electro-mechanical equipment shall be made with either data or alternatives, both of which shall be identified in the Reliability, Maintainability, and Availability Program Plan.

All Major (Class I) engineering changes shall be assessed to determine the need for additional modeling and predictions. Reliability modeling, allocation, and prediction status and analysis for new and redesigned systems, subsystems, and equipment shall be provided at design reviews.

3.5.5.1 Reliability Prediction Methodology

Contractor's reliability predictions for safety and mission critical electronic and mechanical equipment, including Commercial-Off-The-Shelf (COTS), shall be made using parts stress analysis methodology, or intended application field/test data, or failure rates based on worst case part thermal, electrical, and mechanical stress analyses. Reliability predictions shall be made using parts count methodology, intended environment field data, or manufacturer provided reliability data for applicable MDA use environments during the preliminary design stage. All assumptions and associated rationale shall be documented.

3.5.6 Reliability Analyses

Reliability analyses shall be performed concurrently with design so that design deficiencies can be addressed. The following reliability analyses are required on systems, subsystems, and assemblies.

3.5.6.1 Failure Modes, Effects, and Criticality Analysis

The contractor shall conduct a Failure Modes, Effects, and Criticality Analysis (FMECA) to identify potential failure modes of product design for each mission phase and to estimate the effect of failure modes on mission success and safety. A functional FMECA shall be performed for existing and off-the-shelf mission critical items and for immature designs. Once the detailed design is established the FMECA will be updated down to the piece part level failure modes for newly designed and modified mission and safety critical items. Each failure mode shall be assessed and analyzed for the effect at each level of the assembly up to the end item. The failure mode shall be assigned a severity category based on the most severe effect caused by a failure. Where a single failure is undetectable, the analysis shall be extended to assess the effects of secondary failures, which in combination with the first failure, may result in a catastrophic failure condition. The contractor shall initiate a FMECA early in the design phase and update the analysis to reflect affected changes to design configuration. As a minimum, FMECA shall include:

- a. Identification number.
- b. Item/functional identification.
- c. Failure modes and causes.
- d. Mission Phase/Operational Mode affected.
- e. Failure effect.
- f. Severity classification.
- g. Failure detection methods.
- h. Compensating provisions.
- i. Impact on safety, mission success, readiness, and demand for maintenance/logistics support.
- j. Criticality analysis.
- k. Methods and results for obtaining probability of occurrence and recommended actions to preclude or reduce probability of occurrence.

The FMECA shall be scheduled and completed concurrently with the design effort so that designs reflect analysis conclusions and recommendations. When fault trees are used to aid in the FMECA, they shall be documented to the level where recommended action can be taken. The results and current status of FMECA shall be used as inputs to the system engineering process. Results and methods of analysis shall be documented and the FMECA report shall be submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that results and methods of analysis are submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. Failure severity ranking criteria shall be determined as:

- a. Category I (Catastrophic): Can cause death or system loss (e.g., aircraft, satellite, missile, or ship).
- b. Category II (Critical): Can cause severe injury, major property damage, or major system damage, resulting in mission loss.
- c. Category III (Marginal): Can cause minor injury, minor property damage, or minor system damage, resulting in delay or loss of availability, or mission degradation (including loss of redundancy).
- d. Category IV (Minor): Not serious enough to cause injury, or property or system damage, but will result in unscheduled maintenance or repair.

Severity ranking criteria shall be included in FMECA ground rules within the RM&A Program Plan, and coordinated with safety, software, and logistics disciplines. All items with failure modes assigned to Severity Categories I and II shall be itemized on a Mission Critical Items List and maintained with the FMECA report.

3.5.6.2 Fault Tree Analysis

The contractor shall perform, as appropriate, a Fault Tree Analysis (FTA) to support FMECA, design studies, and failure investigations. Beginning with each undesired event, the fault tree shall be expanded to include all credible combinations of events/faults and environments that could lead to the undesired event. Component hardware/software failures, external hardware/software failures, and human factors shall be considered in the analysis. Typical candidates for FTA are functional paths or interfaces that could have critical impact on flight safety, munitions handling safety, safety of operating and maintenance personnel, and probability of error free command in automated systems, in which a multiplicity of redundant and overlapping outputs may be involved. Other candidates for FTA include troubleshooting, repair of products, and prediction and quantifying risk. The FTA results shall be stored in IDE (3.1.5).

3.5.6.3 Finite Element Analysis

The contractor shall use Finite Element Analysis (FEA) as a tool to analytically assess behavior of engineering components, subsystems, and systems under various conditions of use. The FEA is performed to analyze effects of stress (e.g., thermal, physical, and natural frequencies) on parts. Typical candidates for FEA include devices, components, or design concepts that:

- a. Are unproven and for which little or no prior experience or test information is available.
- b. Use advanced or unique packaging or design concepts.
- c. Will encounter severe environmental loads.
- d. Have critical thermal or mechanical performance and behavior constraints.

The FEA results shall be stored in IDE (3.1.5).

3.5.6.4 Sneak Circuit Analysis

The contractor shall perform a sneak circuit analysis on mission critical circuitry affecting system performance and safety where failure results in a Category I or II Severity. Sneak circuit analysis shall identify latent paths, which cause unwanted functions or inhibit desired functions, assuming all components are functioning properly. A list of those circuits and functions analyzed, priorities given each subassembly in the analysis, and supporting rationale for the selections shall be maintained and presented at design reviews. Sneak circuit analysis results shall be stored in IDE [\(3.1.5\)](#).

3.5.6.5 Worst Case Analysis

The contractor shall perform worst case analyses where failure results in a Category I or II Severity. The most sensitive design parameters shall be analyzed, including those subject to variations that could degrade performance. The adequacy of design margins in electronic circuits, optics, electro-mechanical and mechanical items shall be demonstrated by analyses, test, or both. The analyses shall consider all parameters set at worst case limits and worst case environmental stresses. Part parameter values for analyses shall include manufacturing, temperature, cumulative radiation variability, and aging effects of environment. The analyses shall be updated with design changes. The analysis results shall be presented at design reviews and shall be stored in IDE [\(3.1.5\)](#). When a worst case analysis cannot be performed, which may be the case with COTS or Non-Developmental Items (NDI), an alternative approach shall be proposed to the cognizant MDA Program Office.

3.5.6.6 Electrical, Mechanical, and Thermal Stress Analyses

The contractor shall perform electrical, mechanical, and thermal parts/circuits analysis for new designs and proposed design changes. These analyses shall be documented and results reported at design reviews. Electrical, mechanical, and thermal stress analyses may be performed on sheltered equipment, when appropriate, to minimize program risk.

3.5.6.6.1 Thermal Stress Analysis

The contractor shall conduct thermal stress analysis to determine anticipated operational and self-induced temperatures for each mechanical or electrical assembly and component involved in a new design or proposed design change. The stress analysis shall be conducted at worst case environmental and load conditions. The contractor shall ensure assemblies and components are capable of functioning in a temperature environment that does not exceed the item's derated limits, including safety margins. Thermal stress analysis results shall be stored in IDE [\(3.1.5\)](#).

3.5.6.6.2 Mechanical Stress Analysis

The contractor shall conduct a mechanical or structural stress analysis to verify that appropriate margins of safety exist. The stress analysis shall be conducted at worst case environmental and load conditions. Mechanical stress analysis results shall be stored in IDE [\(3.1.5\)](#).

3.5.6.6.3 Electrical/Electronic Stress Analysis

The contractor shall conduct electrical/electronic stress analysis on all new designs, including designs incorporating COTS/NDI, and design modifications to determine from the circuit and the operating conditions of a given application, actual stresses induced on each part. Stress analysis shall be conducted at worst case environmental and load conditions. Unacceptable stress conditions based on derating criteria (MDA-QS-003-PMAP, paragraph 3.2.5) shall be eliminated. Electrical/Electronic Stress analysis results shall be stored in IDE [\(3.1.5\)](#).

3.5.7 Mission Critical Items

The contractor shall use, as a minimum, the following criteria to identify mission critical items:

- a. All Items with failure modes assigned to FMECA Severity Categories I and II.

- b. Impact of potential failure on safety, readiness, mission success, and demand for maintenance/logistics support.
- c. Item has a critical failure mode and a relatively high failure rate.
- d. Item is destroyed or expended upon being activated (one shot device), item performance approaches its design limits, or the item's inherent reliability is degraded by transient stress.
- e. Item's criticality ranking is not mitigated by Pre-Launch Built-In-Test, or other means, to prevent or substantially reduce probability of a hazardous launch.
- f. Application of new technology, new materials, new processes, or advanced state-of-the-art techniques.
- g. Complex production or technical complexity.
- h. Limited source, limited material, or sole source availability.
- i. Item has exhibited an unsatisfactory operation history.
- j. Physical properties of the item are stability sensitive, requiring tight process control.

Methods for controlling and testing mission critical items shall be established and documented. Controls may include supplier surveillance, configuration control/process change reporting, problem reporting, and agreed to tests and inspections. A list of mission critical items and criteria for selection and specific controls shall be stored in IDE (3.1.5). The mission critical items list shall be an input for supplier management (3.13.1.1).

3.5.8 Effects of Functional Testing, Storage, Handling, Packaging, Transportation, and Maintenance

The Government and contractor shall determine the effects of storage, handling, packaging, transportation, maintenance, and repeated exposure to functional testing on hardware reliability.

The Government and contractor shall establish, maintain, and implement procedures to determine by test and analysis, or estimation, the effects of storage, shelf life, packaging, transportation, handling, maintenance and repeated exposure to testing on the design and reliability of a product. The results of this analysis shall be used to support design trade-offs, definition of allowable test exposures, retest after storage decisions, special handling, transportation, packaging, or storage requirements and refurbishment plans.

3.5.9 Controlled and Limited Life Items

The contractor shall establish and maintain a system for determination and identification of controlled and limited life items and criteria for their storage (e.g., First-In-First-Out), control, and use. The system shall:

- a. Include all subsystems, parts, devices, items, or materials, whose useful life expectancy is limited or must be controlled.
- b. Provide for establishing, validating, and updating the life expectancy of each limited life or controlled item.
- c. Prevent issuance, usage, and provide for removal, replacement, review, and disposition of limited life or controlled items, whose specified useable life has expired.

Records shall be maintained that allow evaluation of cumulative stress (time and cycles) for controlled items, starting when useful life is initiated and indicating the project activity that stresses the items. The use of a controlled item whose expected life is less than its mission design life shall be approved by Parts, Materials, and Processes Control Board (PMPCB) (MDA-QS-003-PMAP, paragraph 2.2).

3.5.10 Reliability Growth Test Program

The Government and contractor shall implement a Reliability Growth Test Program, in which systems and subsystems (i.e., hardware and software) are tested under actual or simulated operational conditions. Testing shall be conducted to disclose design deficiencies and defects and enhance system reliability through analysis and correction of defects and verification of corrective action effectiveness. The reliability growth test program and planning shall include methods for achieving reliability growth and for assessing reliability growth progress consistent with program needs, including hardware and program duration. Reliability Growth Test Program and planning are expected to include product availability, test procedures to be used, criteria for correcting failure modes, applicable exit criteria, expected test times and sample sizes, and methods of analyzing test data and reporting results. The Government and contractor are expected to use industry best practices designed to minimize program risks by achieving maximum reliability growth. Reliability growth approach shall be incorporated into the RM&A Program Plan.

The Government and contractor may use MIL-HDBK-189 as additional guidance for implementing a Reliability Growth Test Program.

3.5.11 Accelerated Life Testing

The contractor shall establish and maintain an Accelerated Life Testing program to detect and correct any inherent design and manufacturing flaws and to determine product robustness of safety and mission critical items. The contractor shall establish selection criteria to identify Accelerated Life Testing candidates. Criteria and candidates shall be stored in IDE (3.1.5). Accelerated Life Testing shall be used in an iterative fashion during development, beginning at lower levels of assembly and progressing to higher levels of assembly, until sufficient margins have been verified. Test methods shall include a series of individual and combined stresses applied in steps of increasing intensity (well beyond the expected field environments) until failure or a malfunction is obtained. Failure modes shall be analyzed for root cause and corrective action, as appropriate.

3.5.12 Highly Accelerated Life Test

The contractor shall consider the applicability and feasibility of a Highly Accelerated Life Test (HALT) program to detect and correct inherent design flaws and determine product robustness of safety and mission critical items. HALT shall be considered for newly developed products, re-designed products, and product improvement projects. The contractor shall establish criteria to identify HALT candidates and propose candidates for Government concurrence. The contractor's test method shall include a step-stress approach that progressively increases the stress by inducing thermal, vibration, rapid temperature transitions, and operational cycles to determine the operating and destruct limits of the product and precipitate flaws. Failure modes shall be analyzed for root cause and corrective action. This method shall be repeated until the highest probable limits are found. A HALT program may supplement the Accelerated Life Testing program specified in 3.5.11. A HALT plan shall be incorporated into the RM&A Program Plan (3.5.1), as applicable.

3.5.13 Highly Accelerated Stress Screen

The contractor shall consider the applicability and feasibility of implementing a Highly Accelerated Stress Screen (HASS) program to ensure reliability. HASS shall include conducting simultaneous thermal and vibration stresses to accelerate the precipitation of latent and intermittent defects to a detectable failure. The contractor shall perform a proof-of-screen to ensure that the HASS limits derived during HALT precipitates latent and intermittent manufacturing defects without damaging hardware. The HASS program shall provide feedback into the FRACAS to help determine the most effective screening profiles

and for analysis of defects to determine root cause and corrective action. Feedback shall include latent and intermittent failures, previously undetected or unknown design defects, previously undetected or unknown failure modes, and workmanship defects. A HASS program may supplement the ESS program specified in [3.5.15](#) and [3.12.7](#). A HASS plan shall be incorporated into the RM&A Program Plan ([3.5.1](#)), as applicable.

3.5.14 Process Failure Modes and Effects Analysis

The contractor shall perform a Process Failure Modes and Effects Analysis (PFMEA) to determine potential product failure modes caused by fabrication processes. A PFMEA shall be performed before starting production of ordnance, and safety and mission critical processes. A PFMEA shall be an input in determining process qualification and requalification. Results of PFMEA shall be stored in IDE ([3.1.5](#)). As a minimum, PFMEA shall:

- a. Identify potential product related process failure modes.
- b. Assess potential end user effects of failures.
- c. Identify potential fabrication process causes and process variables on which to focus controls for occurrence reduction or detection of failure conditions.
- d. Develop a ranked list of potential failure modes, thus establishing a priority system for corrective action considerations.
- e. Document or map out the manufacturing or assembly process.

3.5.15 Environmental Stress Screening

The contractor shall establish and maintain an effective Environmental Stress Screening (ESS) Program, so workmanship failures can be identified early and removed from equipment. The program shall include development of ESS profiles based on thermal and vibration surveys, as well as, equipment response analyses. As a minimum, power-on and performance monitoring shall be performed at two levels of assembly. The program shall consider equipment design, part/component technology, and production fabrication techniques.

The contractor shall track effectiveness for each level of screening and establish metrics to support appropriate tailoring of existing screening profiles. The ESS program shall provide feedback into the FRACAS to help determine the most effective screening profiles. Feedback shall include latent and intermittent failures, previously undetected or unknown design defects, previously undetected or unknown failure modes, and workmanship defects. The contractor may use Accelerated Life Testing results as a baseline for determining initial ESS profiles.

The contractor shall document the ESS Program in the RM&A Program Plan. As a minimum, the program shall address:

- a. Description of environmental stress types, levels, profiles, and exposure times to be applied.
- b. Identification of level (i.e., parts, printed wiring assemblies, subassembly, system, and spares) at which testing will be accomplished.
- c. Identification of item performance and stress parameters to be monitored during ESS.

The contractor may use MIL-HDBK-344 and MIL-HDBK-2164 as additional guidance for implementing an ESS program.

3.5.16 Reliability Qualification Test Program/Demonstration

The contractor shall perform Reliability Qualification Testing (RQT) and analysis to determine if specified reliability requirements are achieved. Reliability Qualification Testing shall be performed using items representative of the approved operational configuration, to determine compliance with specified reliability requirements. The contractor shall establish, maintain, and store in IDE [\(3.1.5\)](#) a RQT Plan, which shall include:

- a. Test objectives and selection rationale.
- b. Identification of the item to be tested (with identification of computer programs to be used for the test, if applicable) and the number of test items.
- c. Test duration, appropriate test plan, and test environments.
- d. A test schedule that is reasonable and feasible to permit testing when equipment representative of the approved operational configuration is available.

Detailed test procedures shall be prepared for tests that are included in the RQT Plan. An outline of these tests shall be addressed in the RM&A Program Plan, and details addressed in the Integrated Test and Evaluation Program Plan [\(3.7.1\)](#).

Proposed COTS/NDI shall be subjected to RQT when particular hardware or software has not been used under worst case environments defined by system specification or when there is not sufficient analytical data to support the hardware's allocated reliability to comply with overall system reliability.

The RQT shall be integrated with the overall system/equipment qualification testing program.

3.5.17 Maintainability Modeling, Allocations, and Predictions

The contractor shall develop and maintain a maintainability model (maintainability block diagrams and math models) for each system, subsystem, and lower levels with associated allocation and predictions for all items. These models shall be used to augment systems engineering tradeoff studies. Results of modeling shall be used for maintainability analysis.

The contractor shall allocate quantitative maintainability requirements down to the lowest replaceable unit and ensure inclusion in specifications as design criteria for hardware and diagnostic software. The maintainability requirements shall address servicing, and preventive and corrective maintenance in terms of allowable downtime with consideration for required manpower, skill levels, special tools and test equipment, and diagnostic capabilities.

The contractor shall perform maintainability predictions early in the design phase and update predictions throughout the development effort. Predicted values shall include experience from previous programs. The contractor's predictions shall identify pertinent requirements for accessibility and human factors. Maintainability predictions shall be used in formulating design decisions, maintenance planning, and logistics planning.

The contractor may use MIL-HDBK-470 Designing and Developing Maintainable Products and Systems as additional guidance.

3.5.18 Maintainability Analysis

The contractor shall perform maintainability analysis on subsystems, equipment, and assemblies to the lowest replaceable unit of assembly. Maintainability analyses shall be performed concurrently with design and in conjunction with the reliability effort, so that identified problem areas can be addressed for timely consideration of corrective action. Analysis procedures shall include examination and evaluation of proposed and actual designs, including software, in order to establish the most effective and efficient

design for preventive, progressive, and corrective maintenance, and to identify maintenance resource requirements (e.g., repair parts, skills, and equipment). The analysis shall consider requirements for failure detection and isolation, extent of built-in test capability, input and output media, and results of reliability analyses. When it is determined by the analysis that a proposed or actual design is deficient in meeting qualitative (e.g., access, space, or standardization) or quantitative maintainability requirements, results of the analysis shall drive additional design or redesign.

3.5.19 Maintainability Demonstration

The contractor shall plan and execute a maintainability demonstration to verify system compliance to maintainability specification requirements. The contractor shall use reliability predictions and other pertinent considerations to identify and list the most probable anticipated failures of mission critical real time system functions. The contractor shall use this list to identify a group of candidate maintainability tasks from which a selection shall be made to conduct demonstration tests before deployment.

Maintainability demonstration tests shall verify the capability of planned maintenance activities to meet operational availability/mean-down times required for identified system functions. Tests shall also verify adequacy of fault detection or isolation methods and the ability to achieve lowest replaceable unit replacements or on-site repairs to meet criteria stated in the maintenance plan.

The approach and details of demonstration, including selection of demonstration personnel, technical manuals, and support equipment shall be described in a maintainability demonstration plan that shall be prepared and stored in IDE (3.1.5). The plan shall describe candidate failure scenarios and identify and outline test specification requirements of each candidate individual demonstration.

A maintainability demonstration report shall be stored in IDE (3.1.5). The report shall include data collected, results of data analysis, and conclusions and recommendations. In the event of failure to meet specified maintainability requirements, the report shall present corrective action planned to overcome deficiencies encountered and a schedule for demonstrating effectiveness of changes.

3.5.20 Availability Modeling, Allocations, and Predictions

The contractor shall develop and maintain an availability model (availability block diagrams and math models) for each system, subsystem, and lower levels with associated allocation and predictions for all items. These models shall be used to augment systems engineering tradeoff studies. Results of modeling shall be used for availability assessment.

The contractor shall allocate availability requirements to minimize total ownership costs and to meet program specifications. Availability requirements shall be allocated for all components of the system. Reliability and maintainability requirements shall be derived from and directly support MDA system, subsystem, and assembly availability inherent availability (A_i), and operational availability (A_o). The reliability and maintainability requirements shall be allocated to system, subsystem, and assembly in accordance with paragraphs 3.5.5 and 3.5.17. The contractor shall design for and track both A_i and A_o throughout the life cycle. Operational availability (A_o) shall be monitored for deployed equipment when the contractor is involved in support and maintenance logistics.

Early in the design phase, availability predictions shall be performed for the product and its elements. Availability predictions shall be maintained to reflect current design. The results of availability predictions shall be used as inputs in formulating decisions for product design, safety, maintenance, logistics, and availability analyses.

3.5.21 Availability Assessment

The contractor shall assess product availability beginning with design and test programs and continuing through operational phase. The assessment process shall incorporate and integrate results of reliability and maintainability analyses, engineering analyses, testing, valid operating data from previous generations, and applicable test and usage data for quantitative measurement of product availability.

3.5.22 Reliability, Maintainability, and Availability of Government Furnished Equipment/Information

When the overall system includes components or other elements furnished by the Government, the contractor shall be responsible for identifying and requesting adequate RM&A data on the items. This data shall be used for performing RM&A analyses. When examination of data or testing indicates reliability, maintainability, or availability of Government Furnished Equipment/Government Furnished Information (including COTS or NDI) is inconsistent with RM&A requirements of the overall system, or is unavailable, the cognizant MDA Program Office shall be promptly notified.

3.5.23 Reliability Surveillance of Deployed and Fielded Systems

The Government and contractor shall derive a method to determine and track end items deployed and fielded systems reliability throughout its service life. Surveillance and service life evaluation test [\(3.7.6\)](#), factory test, ground test, maintenance test, health and status tests, Built-In-Test, and flight test data shall be used to determine deployed and fielded systems reliability. Methodology for determining deployed and fielded systems reliability shall be approved by MDA/DE and the cognizant MDA Program Office, and available to MDA/QS. The deployed and fielded systems reliability results shall be briefed during program reviews and stored in IDE [\(3.1.5\)](#) by the contractor.

3.6 Parts, Materials, and Processes Control Program

The Government and contractor shall establish and maintain a Parts, Materials, and Processes Control Program (PMPCP) to ensure selection and use of parts, devices, and materials, including commercial and non-developmental items, meet specified performance, quality, reliability, safety, supportability, and configuration management requirements throughout the life cycle of the system. The program shall include provisions for mitigating the impact of counterfeit parts and parts obsolescence on product integrity.

For safety and mission critical hardware, the program shall have a documented approach for approval, selection, acquisition, handling, packaging, screening, derating, qualification, traceability, standardization, and storage of parts and materials in development and fabrication.

The PMPCP is intended to mitigate risk and enhance probability for mission success for all MDA systems, subsystems, and assemblies.

3.6.1 Parts, Materials, and Processes Plan

The Government and contractor shall develop and maintain a Parts, Materials, and Processes (PMP) Plan. The contractor's PMP Plan shall be developed in coordination with the cognizant MDA Program Office describing the approach and methodology for implementing the PMPCP. The PMP Plan shall describe implementation of MDA-QS-003-PMAP requirements. The contractor's PMP Plan shall be stored in IDE ([3.1.5](#)).

The detailed PMP requirements for all new or modified safety and mission critical products and systems developed for the Missile Defense Agency (MDA) shall be in accordance with MDA-QS-003-PMAP.

3.7 Integrated Test and Evaluation Program

The Government and contractor shall establish and maintain an integrated test and evaluation program to ensure hardware and software meet mission specifications and requirements. The integrated test and evaluation program shall ensure hardware, software, interface, and interoperability capabilities are validated and qualified against requirements identified in the item's configuration documentation. The requirements traceability and verification matrix (3.2.10) shall establish traceability between item requirements and tests used as a basis for validation and qualification decisions. Test programs to be conducted during fabrication and deployment shall be planned, developed, and, as appropriate, exercised during the development phase, so that seamless transitions occur.

The Government and contractor shall develop and maintain integrated test and evaluation program policies, organizational responsibilities, and implementing procedures to ensure:

- a. Effective use and control of test resources, including control, maintenance, and reuse of test data. Test records, including data, shall be stored in IDE (3.1.5).
- b. Establishment and evaluation of objectives, plans, and schedules, including requirements for test documentation, test facilities, test equipment, and test samples. The Government and contractor shall establish uniform test program requirements, guidelines, and instructions for use in test planning.
- c. Methodologies and strategies for testing commercial and non-developmental items to ensure items meet functional and performance characteristics and those characteristics are retained in the procured items.
- d. Development and approval of test plans and procedures.
- e. Test results are reviewed and evaluated to determine whether any appropriate action is required.

The Integrated Test and Evaluation Program includes: Engineering evaluation, qualification, acceptance production assessment, surveillance and service life evaluation, and ground and flight tests. These tests are discussed in the following paragraphs. Additionally, the overall test and evaluation program includes other types of tests discussed elsewhere in this document. These tests include reliability, such as Reliability Growth Testing (3.5.10), Reliability Qualification Testing (3.5.16), and Accelerated Life Testing (3.5.11), tests related to maintainability (3.5.19), tests associated with software development (3.3.2), and tests related to safety (3.14).

3.7.1 Integrated Test and Evaluation Program Plan

The contractor's integrated test and evaluation program shall be described in an Integrated Test and Evaluation Program Plan, which shall be submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. The Integrated Test and Evaluation Program Plan shall be expanded in detail as product and process development progresses. To ensure effective control and use of test resources and complete coverage of testing activities throughout the product's life, planning for hardware, software, and system integration testing shall be included in the Integrated Test and Evaluation Program Plan. The plan shall:

- a. Describe the organization and management of the Integrated Test and Evaluation Program.
- b. Include a summary of tests, including test type, test level, and test objective.
- c. Include schedules for tests, relating test program milestones to major program milestones.
- d. Include schedules for special test facilities/equipment, test items, and test documentation.

3.7.2 Engineering Evaluation Tests

The contractor shall perform engineering evaluation tests to mitigate risk; perform design and development verification ([3.2.11](#)); determine sensitivity of the design to varying levels, combinations, and sequences of electrical, mechanical, and environmental stress; and verify acceptable levels of design and performance margins. These tests may be performed on prototype hardware/software and assemblies/subsystems. Final engineering evaluation tests, used for design and development verification purposes, shall be performed on items that are representative of deliverable hardware and software configurations at the highest assembly levels practical to verify functional compatibility and assess interface interactions at the level tested. A test plan ([3.7.9](#)), test procedure ([3.7.10](#)), and a test report ([3.7.11](#)) shall be prepared for each design verification test and stored in IDE ([3.1.5](#)).

3.7.2.1 Integration Tests

The contractor shall perform integration tests on items that are representative of deliverable hardware and software configurations to verify functional performance and interfaces (e.g., mechanical, electrical, and optical) meet system requirements. These tests shall reflect a systematic, documented method for verifying interface and functional compatibility. Integration tests shall also verify test equipment to unit under test interfaces while proofing test procedures.

3.7.2.2 Interoperability Tests

The Government and contractor shall conduct or support tests to demonstrate compliance with interoperability requirements. This activity shall include testing at various maturity levels and levels of integration/assembly to establish confidence before integrated ground and flight tests. Requirements related to interface requirements, data definition, timing, scale factor compatibility, and error reporting and handling shall be verified through thorough integrated testing at various levels. Verification activities should be closely coupled with systems engineering to ensure implementation of meaningful verification activities. Collectively, these interoperability tests demonstrate compliance with specified interoperability certification criteria.

3.7.2.3 Test-Like-You-Fly

Contractors developing flight and space systems shall conduct engineering evaluation tests for all applicable mission characteristics using a test-like-you-fly (TLYF) approach to demonstrate product meets mission requirements for applicable mission phase and timeline. The TLYF approach shall ensure the test article is evaluated, to the fullest practical extent, in a configuration matching the expected operational configuration and environment. The hardware and software configurations and support equipment shall be well defined, documented, and under configuration management control. Test setups shall be configured to provide expected operational scenarios and operational environments. Final engineering evaluation ground tests conducted before flight testing shall be performed with flight software in an operational ("non-test") configuration to reflect actual software execution paths to be exercised during flight. Any TLYF exceptions shall be identified and documented. Risks associated with these exceptions shall be managed ([3.1.6](#)), and the risk mitigation plans provided before test conduct and approved at test readiness reviews ([3.4.1.9](#)).

3.7.3 Qualification and Requalification Test Program

The contractor shall establish and maintain a program for qualification and requalification of hardware, software, and firmware ([3.3.2.7](#)). The qualification program shall ensure all system elements meet their specification requirements when placed in the operational environment. A requalification decision, including supporting rationale, shall be submitted to and approved by the cognizant MDA Program Office when any of these events occur:

- a. Change in hardware, software, or firmware design.
- b. Change in supplier.

- c. Change in manufacturing processes or plant location.
- d. Interruptions of manufacturing processes greater than 12 months.
- e. Increases in manufacturing rate.
- f. Disqualification of a product.
- g. Changes to equipment, procedures, or software used to test qualified product.

3.7.3.1 Qualification Program Plan

The contractor shall prepare, maintain, and submit a Qualification Program Plan into IDE [\(3.1.5\)](#) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. The Qualification Program Plan shall:

- a. Describe organization and management of the qualification program, including applicable policy statements and management directives.
- b. Identify system elements to be qualified, including reference documentation and qualification methods. Items considered qualified by virtue of previous qualification shall be identified with supporting justification.
- c. Describe entrance and exit criteria for qualification test requirements, test locations and equipment, and system element qualification.
- d. Include schedules for preparing qualification test plans, procedures, and qualification for each system element.

3.7.3.2 Qualification Tests

The contractor's qualification tests shall be performed on configuration items to demonstrate system requirements have been met and ensure associated procedures and processes for fabrication, test, and inspection are satisfactory. Qualification tests shall be performed on samples consistent with deliverable (i.e., consistent with the expected fielded or tested configuration) hardware and software configurations. Qualification tests on items procured from different suppliers shall include samples from every source of each configuration. When a family of items is being qualified, the qualification test specimens shall include a sampling of the full range of values being considered to satisfy design requirements. Environmental qualification tests shall be performed IAW test methods described in SMC-S-016 for space and missile systems and MIL-STD-810 for airborne and ground systems. Qualification tests shall be conducted to the most severe stress levels with margins, identified in system, subsystem, and software specifications to ensure they fully envelope the expected operational levels, sequences, and combinations of stresses. Test facilities shall be capable of providing the required range of operational demands and environmental levels. Mission profile environments and qualification test environments shall be modified to reflect field test data as it becomes available. The qualification test environment shall simulate the operational environment. When qualification tests are conducted at locations other than the contractor's facilities, the contractor shall ensure establishment of controls over the supplier's test program that are equivalent to those for tests conducted within the contractor's facilities.

Test plans [\(3.7.9\)](#) and test reports [\(3.7.11\)](#) shall be prepared for each qualification test and submitted into IDE [\(3.1.5\)](#) and marked for approval by the cognizant MDA Program Office. Notification that test plans and test reports are submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. Test procedures for each qualification test shall be prepared, maintained, and stored in IDE [\(3.1.5\)](#) as part of the Test Readiness Review data package.

The contractor shall evaluate qualification test results to assess complete test coverage and conformance to expected results.

3.7.3.2.1 Qualification by Similarity

Qualification by similarity may be acceptable when hardware has met the following conditions as a minimum:

- a. Used in a similar application in the intended environment.
- b. Based on similar functional characteristics and was tested to stress levels at least as severe as those specified for the part to be qualified.
- c. Tested under program controls commensurate with those imposed on the qualification test program.
- d. Manufactured by the same supplier using similar processes, materials, and quality control, and used in a similar application.

Decisions to qualify based on similarity, including detailed engineering justifications, shall be documented and submitted into IDE [\(3.1.5\)](#) by the contractor. Decisions to qualify are subject to approval by the cognizant MDA Program Office.

3.7.4 Acceptance Tests

The Government or contractor shall conduct acceptance tests to demonstrate the ability of deliverable items to meet specification requirements. Requirements for acceptance test equipment shall be derived from allocated design requirements for the particular item being tested. Whenever possible, acceptance tests shall environmentally stress hardware to maximum conditions expected for all operational events, including transportation and handling. Acceptance tests shall be performed incrementally starting at the component and subassembly levels and progressing to the major assembly and system levels to assure that each item characteristic is completely verified. Acceptance tests shall be performed consistent with fabrication and quality [\(3.12\)](#) plans and procedures, and before items are shipped or delivered [\(3.1.7, 3.4.2.3\)](#). During a developmental ground or flight test program, problems identified during acceptance testing of the item to be flown shall be identified, documented, and the impact reviewed with the cognizant MDA Program Office before the decision to proceed with ground or flight testing.

Contractor acceptance test results shall be stored in IDE [\(3.1.5\)](#).

3.7.5 Production Assessment Tests

For programs that have a production phase, selected parts, devices, materials, and assemblies shall be sampled and a production assessment test performed by the contractor to determine whether production process changes are occurring that will have a detrimental effect on the completed product. These tests shall thoroughly evaluate selected characteristics including application of appropriate stress levels to ensure continued compliance with design criteria. A contractor Production Assessment Test Program Plan shall be developed, coordinated with the cognizant MDA Program Office, stored in IDE [\(3.1.5\)](#), and maintained to indicate selection process, products selected, and the production assessment tests that will be conducted to verify required performance, quality, reliability, and safety aspects of the product are maintained. Parts, components, or assemblies for production assessment testing shall be selected based upon the following criteria:

- a. Susceptibility to environmental conditions.
- b. Effect on mission.
- c. Normal process variability relative to specified tolerances.

- d. Sensitivity to changes in processing variables.
- e. Complexity of manufacturing or production process.
- f. Production quantity and duration.

If an item is produced on more than one processing line or procured from more than one source, sample selection shall cover all lines or sources. The nature of tests, number of test samples selected for each assessment, and frequency of test shall be compatible with complexity of the production process and its controls.

Contractor test plans (3.7.9) and procedures (3.7.10) shall be established and maintained for control of each production assessment test. Results of each production assessment test shall be documented in a test report (3.7.11), which shall be stored in IDE (3.1.5) by the contractor. Actions shall be initiated when data indicates degradation in quality, reliability, or safety of the product or processes used to fabricate or produce it.

3.7.6 Surveillance and Service Life Evaluation Tests

The Government or contractor shall establish and maintain a life cycle surveillance and an accelerated service life evaluation testing program for missile systems and sensors. Surveillance and accelerated service life tests are performed on selected completed items so that timely management decisions can be made to maintain system reliability and operational readiness. These tests shall be performed to:

- a. Provide early detection of aging and degradation of items that may not be revealed during normal maintenance, demonstration, or operational testing.
- b. Permit a continuing assessment of effects of operational environments on the product's quality, reliability, safety, and service life status.
- c. Test parts and materials to assess effects of long term storage.
- d. Identify and establish controls for items that are calendar age, operating time, or cycle time sensitive.
- e. Ascertain aging or environmentally induced trends, service life limits, and other criteria affecting life cycle reliability and operational readiness.

Contractor prepared test plans (3.7.9), test procedures (3.7.10), and test reports (3.7.11) for surveillance and service life evaluation tests shall be prepared, maintained, and stored in IDE (3.1.5).

3.7.6.1 Surveillance and Service Life Evaluation Test Program Plan

A surveillance and service life evaluation test program plan shall be prepared by the Government or contractor. The surveillance and service life evaluation test program plan shall:

- a. Describe the organization and management of the surveillance and service life evaluation test program (e.g., applicable policy statements, management directives, and identification of responsibilities).
- b. Describe the service life in years, and scope of the program including a list of affected items.
- c. Describe maintenance interval, sample selection, handling, and storage.
- d. Describe test requirements including environment, equipment, test interval, and provide or reference test plans and test procedures for each item.

- e. Describe trend analysis to be performed to identify and report trends, which indicate degradation or out-of-specification conditions.

The contractor surveillance and service life evaluation test program plan shall be stored in IDE ([3.1.5](#)).

3.7.7 Ground and Flight Tests

The Government and contractor shall conduct ground and flight testing to execute, demonstrate, and characterize critical aspects of system performance, its subsystems, and its interfaces. Ground and flight test activities include testing of land, air, sea, or space based systems. Testing shall be conducted not only to demonstrate performance of the product but also its interoperability with other affected MDA systems. Ground tests shall be conducted IAW MDA Instruction 3000.07-INS. This ground test CONOPS describes the tailorable processes and activities required to conduct detailed test planning, integration, execution, and analysis of a ground test, and details the nominal timelines for products, tasks, and reviews. Flight test requirements for development, planning, design, readiness, execution, analysis, reporting, and provisioning of MDA test events shall be performed IAW MDA Directive 3002.03. Specific flight test activities are described in the BMDS Test CONOPS document. Test execution comprises a multitude of activities, using specific terminology, and following prescribed processes. The Government and contractor shall use MDA Manual 9420.03 which defines processes, nomenclature, and activities required to be performed or used in executing an MDA test event. Government and contractor test plans and test procedures shall include the requirements specified in [3.7.9](#) and [3.7.10](#) as a minimum.

It is MDA policy that international participants and observers will be included in test events when appropriate. International test events shall be conducted IAW MDA Directive 3100.01. The decision to involve an international partner in a test event is an MDA corporate decision. Testing must be conducted IAW applicable international cooperation agreements.

The Government and contractor shall support the MDA executive level process for test reviews and post test reporting IAW MDA Directive 3200.03. Test reviews provide assurance to the MDA Director (MDA/D) that the test design, planning, and execution activities provide a high probability of test mission success. Post test reports provide timely test and assessment results, to provide evidence that data collection and analysis support the evaluation of test objectives, and to facilitate the systems engineering process for continued system development and fielding.

The Government and contractor shall support the MDA BMDS discrepancy reporting and test event certification processes.

3.7.7.1 Test Risk Management Program

The Government shall document and report test risks separately from programmatic risks ([3.1.6](#)). The Test Risk Management Program is meant to complement, not duplicate risk management activities specified in MDA Risk Management Instruction 3058.01-INS. The nature of BMDS test event risks requires that they be assessed differently. Test Risks are those risks that can impact the Test Baseline and are addressed and managed by MDA/DT as part of the Test Baseline Working Group. Risks that are short lived and specific to a particular test event (i.e., flight or ground tests) are addressed in the Mission Readiness Working Group. The test specific risk process is documented in the MDA Test Risk Management Plan.

3.7.7.2 Critical Test Gate Process

The contractor shall conduct a series of informal working level data reviews that gate critical steps in the build up and check out of ground and flight test units. These working level review meetings shall include representatives from all affected engineering, test, and safety organizations and allow for participation by the cognizant MDA Program Office or designated representative(s).

The contractor shall conduct test process reviews with specific predetermined exit criteria at gating points

in the test asset build up process to ensure adequate proofing of test equipment and test software before subjecting actual flight hardware to the associated test. Test processes and results shall be reviewed to verify proper performance of hardware and software (i.e., qualification tests, acceptance tests, electromagnetic tests, and live battery tests) prior to flight unit assembly and test. The Government and contractor shall verify the flight or ground configuration is IAW the approved test configuration. The Government and contractor shall be accountable for tracking progress through this gate process and ensure the impact of any liens incurred through this process are understood, documented, and resolved before the test event.

3.7.7.3 Post Test Performance Analysis

The Government and contractor shall conduct a comprehensive post test evaluation addressing all aspects of mission conduct and include not only specification compliance of the system but also system robustness and margin. Results that are analyzed shall include all data from command and control systems operations, system performance during ground and flight tests, performance of all associated subsystems, target, and ground support equipment operation. Analysis shall verify environments (e.g., shock, acoustics, and loads) are within analysis expectations. Any out-of-family performance, anomalies, and nonconformances for the test unit and critical ground systems shall be identified and assessed. The contractor shall implement a process that captures lessons learned [\(3.1.5\)](#).

3.7.7.4 Failure Review Process

In the event of failures (ground or flight equipment) during MDA scheduled tests, the Government and contractor shall convene a formal failure review process and board with technical Government and contractor representation to ensure top level management concurrence with the identified root cause and corrective action as defined in MDA Manual 3000.05-M, BMDS Test Failure Initial Response. A failure review team consisting of Government and contractor technical experts shall be assembled to investigate all failures. Early in the process, fault trees shall be defined by the team. All branches of the tree shall be investigated and closed only after persuasive technical justification has been reached. Where practical, fault insertion testing shall be performed to demonstrate all aspects of the failure can be reproduced by the most likely failure mode. For flight failures, closure actions shall be approved by a MDA top-level management FRB, which includes experienced individuals from both Government and contractor organizations. Corrective action shall be defined and approved by the MDA FRB before design implementation. If all fault tree branches cannot be ruled out, corrective action to address all remaining potential fault mechanisms shall be implemented.

Contractor FRB review results shall be stored in IDE [\(3.1.5\)](#).

3.7.8 Modeling and Simulation

The Government and contractor may use Modeling and Simulation (M&S) [\(3.2.14\)](#) before, during, and after completion of ground and flight tests, as a method of demonstrating critical aspects of performance of the system, subsystems, and interfaces. Models and simulations shall be verified, validated, and accredited. The M&S outputs shall be reported, correlated, and validated against actual test data to increase confidence levels, reduce test costs, and support Government evaluation decisions. Verification is the process of determining that a model or simulation implementation accurately represents the conceptual description and specifications. Validation is the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses. Accreditation is the formal certification that a model or simulation is acceptable for use for a specific purpose.

3.7.9 Test Plans

The Government and contractor shall develop and maintain a test plan for each test. Test plans shall include:

- a. Identification of the item and quantity to be tested.

- b. Test objectives.
- c. Test requirements; including parameters to be measured, environments to be simulated, test time, facilities, test and measurement equipment, and software.
- d. Requirements for data collection, analysis, and reporting.

3.7.10 Test Procedures

The Government and contractor shall develop and maintain procedures for each test. Test procedures shall include:

- a. Characteristics to be tested or measured, including tolerances.
- b. Input and range of test parameter values, including tolerances.
- c. Identification of test and measuring equipment, tools, jigs, fixtures, recording equipment, and supporting software.
- d. Identification of special equipment or facilities.
- e. Method to be used in test performance, including sequential steps.
- f. Verifications to be made before conduct of test.
- g. Instructions for data recording.
- h. Actions to be taken in the event of test interruptions.
- i. Pass or fail criteria.
- j. Applicable safety precautions for personnel and facility protection.
- k. Diagram or detailed description of the test setup, such as interconnection information, relative equipment placement, mounting of sensors, and grounding points.
- l. Parts, devices, and material protection requirements.

3.7.11 Test Reports

The Government and contractor shall document and retain test data, including test conditions, significant events, and problems in a report. Deviations from required test equipment configuration, test item configuration, and test environment shall be documented and reconciled.

Test reports shall include:

- a. A reference to the applicable test plan and procedures.
- b. Copies of waivers, deviations, engineering change requests, and failure reports pertaining to test.
- c. Identification of significant events, problems, and any variances from the test procedure.
- d. Identification of specific test equipment used, including the due date for its next calibration.
- e. Results of data analysis, failure diagnosis, conclusions, and recommendations.

- f. Reconciliation of test item configuration and the item's configuration baseline.
- g. Reconciliation of actual test environment with the planned test environment.
- h. Reconciliation of the accumulated environmental stress, with predicted life.

3.8 Test, Measuring, and Diagnostic Equipment and Standards

The contractor shall establish and maintain a system for definition, selection, design, evaluation, approval, maintenance, calibration, use, and control of Test, Measuring, and Diagnostic Equipment and Standards (TMDES) necessary to verify adequacy of processes and product conformance during all program phases. The system shall comply with requirements of ANSI/NCSL Z540.3, Requirements for the Calibration of Measuring and Test Equipment. Test, measuring, and diagnostic equipment and standards include test and inspection equipment, test support equipment, gages, and equipment used to monitor and control production processes. The TMDES also include, production tools, jigs, fixtures, and personally owned measuring equipment used to measure, test, verify, calibrate, diagnose, or otherwise examine materials, supplies, and equipment to determine compliance with product and process specifications.

Contractors who operate and maintain calibration laboratories or subcontract to outside calibration laboratories shall ensure compliance with requirements of ISO/IEC 17025:2005(E), General Requirements for the Competence of Testing and Calibration Laboratories.

3.8.1 Selection and Design

The contractor or calibration laboratory shall establish and maintain a system for selection, design, and evaluation of Test, Measuring, and Diagnostic Equipment (TMDE), including related software used to verify conformance to product and process specifications. The selection and design system shall give preference to selection of Commercial-Off-The-Shelf (COTS) equipment, standards, software, fixtures, cables, and materials rather than items that are unique or proprietary. The TMDE shall have the accuracy, range, resolution, repeatability, reliability, and stability required so that the total uncertainty in any measurement process does not exceed 20 percent of the tolerance of the characteristic being measured. For single limit parameters, the required accuracy shall be specified. If measurement or calibration accuracies cannot be achieved due to technology limitations, a request for variance ([3.10.4.6](#)) shall be submitted into IDE ([3.1.5](#)) and marked for approval by the cognizant MDA Program Office. Notification that the request for variance is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.8.1.1 Test, Measuring, and Diagnostic Equipment Configuration Documentation

The contractor shall develop and maintain configuration documentation for uniquely designed TMDE items and test stations. The maximum permissible variation among test stations shall be specified in its configuration documentation. The configuration documentation package shall be controlled IAW [3.10](#) and shall include:

- a. Calibration procedures.
- b. Operating instructions.
- c. Programming instructions.
- d. A Measurement Accuracy Report.
- e. Configuration documentation for the TMDE including top assembly drawings, interface control drawings, lower level design drawings, and specifications.
- f. Configuration documentation for any developed software including source codes for, but not limited to operating system, test executive, test, calibration, diagnostics, test libraries, and instrument drivers.

3.8.1.2 Evaluation of Test, Measuring, and Diagnostic Equipment

Test, Measuring, and Diagnostic Equipment used to verify conformance to product and process documentation shall be evaluated to ascertain the item will provide required inputs, loading, and

measurement capabilities. Evaluation shall consist of preliminary uncertainty analysis and verification testing.

- a. Preliminary uncertainty analysis shall compare proposed TMDE capabilities with product or process parameter tolerances. The TMDE capabilities shall be based on equipment uncertainty information specified by manufacturers of commercial equipment, data available from previously used equipment, and engineering estimates for new design equipment. The TMDE uncertainty for each input, load, and measurement shall be compared with each respective specification tolerance to calculate accuracy ratios. For new TMDE designs, preliminary uncertainty analysis shall be performed concurrent with design release.
- b. Verification testing shall be conducted on the first unit of TMDE containing a new design to determine inherent uncertainties and to verify uncertainties that cannot be verified in preliminary uncertainty analysis. Verification testing shall also be conducted on commercial equipment where preliminary uncertainty analysis was inconclusive. Verification testing shall be done under required environmental operating conditions. These tests shall be of sufficient scope and duration to demonstrate compliance with accuracy and repeatability requirements.

The TMDE uncertainty obtained from any verification testing shall be used to complete the uncertainty analysis. Records shall be kept of all uncertainty analyses and verification testing results and stored in IDE (3.1.5).

3.8.1.3 Proofing, Qualification, and Correlation

The uniquely designed TMDE or test stations shall be proofed and qualified to ensure effectiveness in measuring the product's compliance to configuration documentation. Proofing and qualification (3.7.3.2) shall be performed under actual operating and environmental conditions to verify completeness and adequacy of equipment, software, material, personnel training, and documentation related to station calibration, station maintenance, and product verification. Additionally, proofing and qualification shall include, but not be limited to, verification of supporting test disciplines covering test performance, calibration performance, maintenance performance, environmental controls, configuration controls, security, and safety. The contractor shall conduct accuracy, reproducibility, repeatability, and trend analysis to assess uniformity, consistency, and stability of the TMDE or test station. The TMDE or test stations shall be re-proofed and re-qualified if changes or modifications affect functionality and usage. The contractor shall notify the cognizant MDA Program Office and designated representative(s) of operational proofing and qualification events to allow for Government participation. Before use, operational proofing and qualification results shall be documented and stored in IDE (3.1.5).

The contractor shall perform correlation to detect and correct conditions contributing to significant variation in results among like or similar test stations. Correlation of test stations shall be performed on a periodic basis to assure repeatable test results. The contractor shall define criteria for performing re-correlation of test stations. Methods and results for each correlation analysis shall be documented and stored in IDE (3.1.5).

3.8.2 Calibration and Maintenance

The contractor shall establish and maintain a system for calibration and maintenance of TMDES that is in compliance with ANSI/NCSL Z540.3. Calibration laboratories operated and maintained by the contractor or subcontracted by the contractor shall ensure compliance with the requirements of ISO/IEC 17025, and as supplemented by the following paragraphs.

3.8.2.1 Calibration and Maintenance Procedures

The contractor or calibration laboratory shall document and maintain procedures for calibration and maintenance of TMDES. Calibration and maintenance procedures shall be stored in IDE (3.1.5). In addition to ANSI/NCSL Z540.3 and ISO/IEC 17025 requirements, calibration and maintenance procedures shall specify or contain:

- a. Description of preparations that must be made before calibration is started.
- b. Descriptions or diagrams of the equipment setup, as necessary.
- c. Environmental conditions required and stabilization period.
- d. Step-by-step instructions for performing calibration and maintenance activities.
- e. Data to be recorded, reports or certificates to be prepared, and method of analysis.

3.8.2.2 Records and Analysis

Records shall be retained for the calibration and maintenance system. In addition to applicable ANSI/NCSL Z540.3 and ISO/IEC 17025 requirements, records and analysis requirements, data shall also be recorded documenting the condition of nonadjustable or fixed value equipment. Calibration data shall be analyzed in order to identify trends indicating deterioration and to provide for revision of intervals to ensure continued accuracy and reliability of TMDES, where reliability is defined as the probability the item will remain in tolerance throughout the established interval. Individual records used to maintain the calibration system shall be stored in IDE [\(3.1.5\)](#).

3.8.2.3 Out-of-Tolerance Conditions

As a supplement to ANSI/NCSL Z540.3, the contractor shall remove and segregate, where practical, nonconforming TMDES from service. When TMDES are found to be nonconforming during calibration, an analysis shall be performed to determine the impact on product and the need for subsequent corrective action. When the analysis indicates the nonconformance could recur, corrective action shall be performed immediately to identify and correct root cause of the problem. The contractor or calibration laboratory shall maintain a record of the out-of-tolerance condition, significance of the nonconformance, and the corrective actions taken. The cognizant MDA Program Office shall be informed of occurrences affecting MDA products and a record documenting the event, subsequent analyses, and any actions taken shall be stored in IDE [\(3.1.5\)](#).

3.8.2.4 Calibration Standards and Reference Materials

Calibration standards and reference materials used for calibrating TMDES items shall have the accuracy, stability, range, and resolution required for intended use. The collective uncertainty of the individual or grouping of calibration standards and reference materials shall not exceed 25% of the acceptable tolerance for each characteristic being calibrated. Calibration standards and reference materials held by the contractor or calibration laboratory shall be used for calibration or verification of working level TMDE only, unless it can be demonstrated their performance as standards has not been invalidated. Requests for variance [\(3.10.4.6\)](#) from these requirements, with supporting justification, shall be submitted into IDE [\(3.1.5\)](#) and marked for approval by the cognizant MDA Program Office. Notification that the request for variance is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.8.3 General Test, Measuring, and Diagnostic Equipment and Standards Requirements

The contractor shall establish and maintain a system to control use of TMDES in compliance with ANSI/NCSL Z540.3 and the following paragraphs. The system shall provide for accountability for use both inside and outside the calibration laboratory and shall ensure accuracy and integrity of resulting measurements and test data.

3.8.3.1 Intervals and Recall

The contractor shall calibrate and maintain TMDES at periodic intervals established on the basis of stability, purpose, and degree of usage. The contractor shall establish and maintain an interval

adjustment system that is based upon a verifiable statistical methodology appropriate for the type of equipment being controlled. Calibration intervals may be lengthened when results of preceding calibrations provide definite indications such action will not adversely affect confidence in accuracy and reliability of TMDES. The system for establishing calibration intervals, adjustments, and subsequent revisions, including reliability targets, shall be stored in IDE (3.1.5).

The contractor shall provide for mandatory recall and calibration of TMDES within established intervals. The recall system shall provide for accountability information, current calibration status, location and identification of all TMDES, and indicate when all items are due for calibration, service or functional check, or out-of-tolerance condition.

3.8.3.2 Labeling

Calibration labels, traceable to the calibration organization and to the item's calibration record, shall be affixed to TMDES. The contractor shall establish traceability between TMDES items and their respective calibration records. When a test or inspection station is calibrated as a single unit, a label shall be affixed to the console frame or similar permanent, common item. The TMDES not requiring calibration shall be clearly identified as such. The contractor shall ensure access and use of labels is controlled and restricted to authorized personnel.

3.8.3.3 Sealing for Integrity

Tamper resistant seals shall be affixed to operator accessible controls or adjustments affecting calibration of TMDES items or test stations. For equipment with removable covers, any internal controls or adjustments are also considered to be operator accessible. Seals shall be designed to destruct on entry. If the seal has been broken, lifted, or is otherwise suspect, the item shall be considered suspect and treated as if the calibration is void. Cabinets, consoles, doors, access covers, and equipment cases may be secured and sealed in lieu of sealing individual equipment controls and adjustments or test station components, provided operator accessibility is prevented. The contractor shall establish and maintain a system for ensuring that access to and use of seals is controlled and restricted to authorized personnel.

3.8.3.4 Removal of Test, Measuring, and Diagnostic Equipment and Standards

Test, Measuring, and Diagnostic Equipment and Standards not calibrated and maintained IAW established intervals shall be physically removed from service where practical, or appropriate tags shall be attached. The TMDES items found with broken calibration seals or suspected to be malfunctioning because of mishandling, damage, misuse, or unusual results shall be removed from service or tagged and controlled to prevent further use.

3.8.3.5 Test Station Logs

The contractor shall establish and maintain test station logs to record station history including station operational proofing, calibration of equipment, seal integrity, equipment servicing and replacement, explanations for modifications and breaks-of-station, and any other pertinent information on unusual events or circumstances. Log entries shall be signed or otherwise traceable to the person making the entry and shall include date and time of the event.

3.9 Interface Management

The Government and contractor shall establish and maintain an interface management program (includes hardware and software) that provides for an effective system integration, interoperability ([3.2.5](#) & [3.7.2.2](#)), accountability, and timely dissemination of related changes. The interface management program shall establish methods for identification, controlling, verification, and flow down of interface requirements found in documents (e.g., BMD System Specification and element interface control documents), drawings, software, data, and other Technical Data Package (TDP) elements. The program shall also control or address interfaces in subcontracted items, Government Furnished Equipment or items, and facilities. The Government will develop interface requirements and interface design documentation as specified in MDA Ballistic Missile Defense Systems Engineering Systems Engineering Plan. The contractor shall coordinate interface management activities with the cognizant MDA Program Office. The cognizant MDA Program Office will coordinate interface management activities with MDA/DE and MDA/BC.

3.9.1 Interface Control Plan

The contractor shall establish and maintain an Interface Control Plan (ICP) that provides effective processes for integration, interoperability, and compatibility of all mechanical, electronic, electrical, optical, software, data interfaces, internally, and, as applicable, externally with other MDA system interfaces as required in the BMD System Specification. The ICP shall define the requirements to manage and control mechanical, electronic, electrical, and optical Interface Control Documents and Drawings (ICD), software Interface Design Descriptions (IDD), Interface Requirement Specifications (IRS), data interfaces, including BMDS, MDA element, and system interfaces. The ICP shall clearly delineate interface responsibilities flowed down to suppliers. The ICP shall be stored in IDE ([3.1.5](#)).

3.9.1.1 Interface Control Plan Development

The contractor, in coordination with the cognizant MDA Program Office, shall develop the ICP, identifying roles and responsibilities for each activity involved in the interface management system including schedule and milestones for completion of ICP activities. Additionally, the ICP shall contain:

- a. Identification of Internal and External Interface Requirements. When identifying internal and external interfaces, the contractor shall take a top down approach from the most generic to the most specific. Interfaces shall be classified as either internal or external. Internal interfaces are defined by mechanical, electronic, electrical, and optical ICDs, software IRSs, and IDD that are internal to each individual system. Internal interfaces are synonymous to correlation interfaces. External interfaces are defined by mechanical, electrical, and optical ICDs, software IRSs, and IDD that control interoperability, interchangeability, and compatibility between subsystems and other systems. External interfaces are synonymous to coordination interfaces. Internal and external interfaces shall be defined, identified, and documented at all levels affecting coordination and correlation. Resulting interfaces shall be defined and managed according to the ICP.
- b. Identification of all Interface Documentation (ID). The ICP shall identify all configuration IDs used to manage and control internal and external system interfaces.
- c. The ID Incorporation. The ICP shall define methods for flowing ID into TDPs.
- d. Verification Process. The ICP shall define the verification process and methods used to ensure all internal and external interfaces meet specified requirements. Verification of internal and external interfaces shall be performed at the lowest level where the interface characteristic can be completely verified. Interface requirements shall be included in the requirements traceability and verification matrix [3.2.10](#) and software verification [3.3.3.2](#).

3.9.2 Interface Documentation

The contractor shall develop, maintain, and control the following Interface Documentation (ID) IAW [3.10](#). The IDs shall be developed according to requirements flowed down from top level requirements and shall include:

- a. Interface Control Documents and Drawings, which shall define and establish functional, electrical, mechanical, optical, and data interface requirements. Interface Control Drawings define detailed external and internal interface dimensions, parameters, characteristics, requirements, and configurations.
- b. Interface Requirement Specification, which shall define and establish external and internal software and data interface requirements for various system, computer, processor, and data interfaces.
- c. Interface Design Description, which shall define and establish detailed design for one or more interfaces incorporated into software configuration items, components, and units. The IDD documents the design for those interfaces specified by IRSs.

Interface documentation (e.g., ICD, IRS, and IDD) shall be submitted into IDE ([3.1.5](#)) and marked for approval by the cognizant MDA Program Office. Notification that the interface documentation is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.9.3 Interface Control Working Groups

The contractor shall develop an Interface Control Working Group (ICWG), which manages interfaces to ensure integration and compatibility within the contractor's system(s) and to external systems. The ICWG membership shall include representatives within the contractor's organization, affected suppliers, and a technical Government representative. The ICWG members shall be selected based on their knowledge and experience and shall have authority to act for their respective organizations. Records of ICWG minutes and actions shall be stored in IDE ([3.1.5](#)). The contractor shall also provide representation to the cognizant MDA Program Office level ICWGs.

The contractor ICWG shall:

- a. Plan, schedule, execute interface definition activities, and resolve interface issues.
- b. Ensure their actions do not affect safety, quality, or mission assurance.
- c. Provide technical support to other system level ICWGs.
- d. Communicate all issues related to interface control to program management representatives and, as necessary, other ICWGs.
- e. Ensure the design meets interface requirements and coordinate proposed interface changes to the TDP.
- f. Coordinate with affected organizations to discuss and resolve technical problems or issues.

3.9.4 Interface Change Notice

The contractor shall generate an Interface Change Notice (ICN) to incorporate ICWG approved changes resulting from integration incompatibility issues and changes to ID. The purpose and rationale for the requested change will be detailed in the ICN. All ICNs must include the exact text, figure, or drawing change to be incorporated and will be related to the existing ID. The ICN shall be submitted to the appropriate change board for disposition and classification. Approved ICNs shall be processed IAW configuration management change control process ([3.10.4](#)) and stored in IDE ([3.1.5](#)). This process shall

be defined in the Configuration Management Plan ([3.10.1](#)). An ICN, its contents, or any attachments thereto, shall not be used to alter or attempt to alter existing contractual obligations.

3.10 Configuration Management

The Government and contractor shall establish and maintain a Configuration Management (CM) system for control of all configuration documentation, physical media, and physical parts representing or comprising the product, which includes all hardware, software, and firmware. The Government's configuration management system shall be IAW BMDS SEP. The contractor's configuration management system shall consist of these elements:

- a. Configuration management and planning ([3.10.1](#)).
- b. Configuration identification ([3.10.3](#)).
- c. Configuration change management ([3.10.4](#)).
- d. Configuration status accounting ([3.10.5](#)).
- e. Configuration audit ([3.10.6](#)).
- f. Configuration management of digital data ([3.10.7](#)).

3.10.1 Configuration Management Plan

The contractor shall develop and maintain a CM Plan. The CM Plan shall be submitted into IDE ([3.1.5](#)) and marked for approval by the cognizant MDA Program Office. Notification that the plan is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. The CM Plan shall include:

- a. General product definition and scope.
- b. Description of CM activities and procedures for each major CM function, including:
 - 1) Configuration planning and management.
 - 2) Configuration identification.
 - 3) Configuration change management.
 - 4) Configuration status accounting.
 - 5) Configuration verification and audit.
 - 6) Configuration management of digital data.
- c. Organization, roles, responsibilities, and resources.
- d. Programmatic and organizational interfaces.
- e. Deliverables, milestones, and schedules.
- f. Supplier flow down.

The contractor may use MIL-HDBK-61A as additional guidance for CM.

3.10.2 Supplier Configuration Management

Supplier's CM performance shall be the responsibility of the contractor and reflected in the contractor's CM documentation. The contractor shall monitor suppliers via data reviews, configuration change management activity, design reviews, product test results, configuration audits, and supplier evaluations.

3.10.3 Configuration Identification

The contractor shall establish and maintain a system for configuration identification. The system for configuration identification shall consist of Configuration Item (CI) selection; determination of types of configuration documentation required for each CI; and issuance of numbers and other identifiers affixed to the CI and its associated technical documentation. Configuration identification for Commercial-Off-The-Shelf (COTS) and Non-Developmental Items (NDI) shall be at the level of detail required to support procurement.

3.10.3.1 Product Information

The contractor shall establish and maintain a system for development and control of product information consisting of configuration documentation and operational information. Configuration documentation defines functional, performance, and physical attributes of a product which includes design and implementation decisions applicable to the CI and product. Operational information is derived from configuration documentation. Operational, build, and test data includes information necessary to use and operate the product (e.g., operating procedures) and other documentation necessary to service and maintain the product.

3.10.3.2 Product Structure and Configuration Item Selection

The contractor shall define the product composition, as part of the technical data package, (i.e., relationship and quantity of parts that comprise the product) as determined from its configuration documentation.

The product structure shall consist of a representation of the breakdown hierarchy (i.e., product tree/pyramid) of a complex product, from the top down to the lowest level CI or Software Configuration Item (SCI). Each level shall reference associated configuration documentation (e.g., engineering drawings, bill of material, specifications, software requirements, design requirements, and processes/procedures). The product structure shall also indicate the top-down relationships among various parts that make up the product and the quantity of each. Product structure shall be considered complete when all parts and configuration documentation are included.

The contractor shall use product structure in determining recommended CIs and Configuration Identification level(s) at which to apply CM, and to evaluate the impact(s) of proposed changes to the product.

The contractor shall submit the final CI selection into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that the final CI selection is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.10.3.3 Product Identifiers

The contractor shall assign unique identifiers to all products so that one product can be distinguished from other products, one configuration of a product can be distinguished from another, the source of a product can be determined, and the correct product information can be retrieved.

The product and each of its component parts shall be assigned unique identifiers, as follows:

- a. Parts of the product developed by, or acquired from, suppliers shall retain unique identifiers assigned by the supplier.

- b. When special requirements are applied to a product, the contractor shall provide a unique identifier, in addition to the supplier's identifier, to correlate the part to its specification requirement.
- c. When a change is applied to a product or part of a product, its descriptive configuration documentation shall be updated to reflect the change. The unique identifier assigned to a product or part, and the marking on the part itself, shall be changed to distinguish one configuration of the product from another, when any:
 - 1) New or updated part is no longer interchangeable functionally or physically with the previously delivered part or with the previous undelivered parts that will remain in a different configuration.
 - 2) New part requires new or revised testing, maintenance, repair, training, operating procedures, equipment, or software.
 - 3) Part is altered, selected, or is a source controlled item per ASME Y14.24.
 - 4) Updated part has different application, use, or safety or other restrictions.
- d. When a repair part within a product is changed so that it is no longer interchangeable with its previous version, it shall be assigned a new identifier. Specifically, the contractor shall re-identify the next higher assembly and all subsequent higher assemblies up to and including the level at which interchangeability is re-established, or an identifiable end product (against which configuration changes are tracked) is reached.

3.10.3.3.1 Unique Software Identifiers

Unique software identifiers shall be assigned by the contractor for each software product and for software products used in the software engineering and test environments. The software identifier shall include the version of the entity. Software units shall be assigned a name or number that is unique within the software product. The marking and labeling of software shall follow these parameters:

- a. The software identifier shall be embedded in the source and executable code header.
- b. Each software medium shall be labeled with the supplier's code/name identification and software identifiers of the software product it contains. If it is impracticable to include all software identifiers, the medium shall be labeled with a reference to an embedded list (e.g., a readme.txt file) containing the identifiers.
- c. Wherever possible, electronically reprogrammable hardware with resident software shall be labeled with the software identification number of the resident software and the hardware part number.

3.10.3.3.2 Identifying Individual Units of Product

The contractor shall assign each individual unit of a product a unique product unit identifier (i.e., serial number) when there is a need to distinguish one unit of the product from another unit of the product. When a product is modified, the contractor shall retain the product's original product unit identifier (i.e., serial number) even though its part identifying number is altered to reflect a new configuration.

3.10.3.3.3 Identifying Groups of Units of a Product

The contractor shall assign a series of like units of a product a unique product group identifier (i.e., lot or batch number) when it is unnecessary or impracticable to identify individual units but necessary to correlate units to a process, date, event, or test.

The lot or batch number shall use an identifier as a base. When a product is modified, it shall retain its original product group identifier even though its part identifying number is altered to reflect a new configuration, unless the modification involves a new grouping.

3.10.3.3.4 Department Of Defense Item Unique Identification

The Government and contractor shall provide an Item Unique Identification (IUID) for MDA items IAW MDA Directive 4161.02 as directed in BMDS SEP. Item Unique Identification application is specified in DOD Directive 8320.03 and DOD Instruction 8320.04. The IUID standards will enable on demand information in a net centric environment, which is an essential element in the accountability, control, and management of DOD assets and resources. Item Unique Identification shall be marked IAW MIL-STD-130.

3.10.3.4 Document Identification

The contractor shall uniquely identify all documents reflecting product performance, functional or physical requirements, and other product information, so they can be correctly associated with the applicable configuration baseline of the product.

3.10.3.5 Configuration Baselines

Contractor configuration baselines shall be established, which identify and describe attributes of a product at a point in time, and provide a known configuration to which changes are addressed.

3.10.3.5.1 Establishing Configuration Baselines

The contractor shall establish and maintain a system to include:

- a. What configuration baselines are to be established.
- b. When and how configuration baselines are defined.
- c. The process for assuring document and file integrity.
- d. The authority to approve configuration baselines and changes.
- e. If and when change authority will transfer.
- f. The process by which proposed changes will be dispositioned.
- g. Configuration baselines traceable to their predecessors and successors.

The contractor shall review any document or data set being considered for inclusion in a configuration baseline to ensure the document or data set is complete, consistent, accurate, and valid. Configuration change management ([3.10.4](#)) shall be used in managing changes to configuration baselines.

3.10.3.5.2 Types of Configuration Baselines

The configuration of any product, or any document, plus the approved changes to be incorporated shall be considered the current baseline.

As determined by the cognizant MDA Program Office, the contractor shall establish and maintain the following types of configuration baselines:

- a. Functional Baseline: Defines the required system functionality, describes the functional and interface characteristics of the overall system, and includes the verification method required to demonstrate

achievement of those specified functional characteristics. The functional baseline shall be under configuration control at the conclusion of the System Functional Review (3.4.1.4) and verified with a System Verification Review (3.4.1.10) and a Functional Configuration Audit (FCA) (3.4.1.11).

- b. **Allocated Baseline:** Defines the CIs making up a system, and allocates system function and performance requirements across lower level CIs. The allocated baseline shall include all functional and interface characteristics allocated from the top level system or higher level CIs, derived requirements, interface requirements with other CIs, design constraints, and the verification required to demonstrate the traceability and achievement of specified functional, performance, and interface characteristics. The contractor is responsible for assuring allocated requirements provided to suppliers are consistent with the functional and performance requirements. The allocated baseline shall be under configuration control at the conclusion of each CI's (hardware and software) Preliminary Design Review (PDR) (3.4.1.7).
- c. **Design Release Baseline:** The contractor shall establish and maintain a process for initial release of design information and for release of approved engineering changes to the design information. Once design information is released, it shall become part of the design release baseline controlled by the developing activity.
- d. **Product Baseline:** Defined by the complete set of current product configuration documentation. The initial product baseline shall be under configuration control at conclusion of each configuration item's Critical Design Review (CDR), culminating in an initial system product baseline established at the system level CDR. The system product baseline is finalized and validated at the Physical Configuration Audit (PCA) (3.4.1.13).
- e. **Additional Operational Phase Baselines:** Supplemental baselines may be required that are either location oriented views (extracts) of the product configuration baseline, or that add supplemental information of concern to the product operation, support, or maintenance. These baselines are typically identified and controlled at operational sites.

3.10.3.6 Interface Control

All external interfaces shall be controlled IAW 3.9.

3.10.4 Configuration Change Management

The contractor shall establish and maintain a configuration change management system. The system shall identify the need for a change, document change impact, evaluate and coordinate the proposed change (including approval/disapproval), incorporate the approved change in the product and its related configuration documents, and implement variances from configuration baseline requirements. The contractor shall provide the Government access to their electronic configuration management system.

3.10.4.1 Classifying Changes

The contractor shall classify requested changes to ensure appropriate levels of review and approval. The contractor shall use the following criteria to differentiate between Class I and Class II changes.

3.10.4.1.1 Class I Engineering Change

The contractor shall classify a requested change as Class I if:

- a. An engineering change to the requirements of baselined configuration documentation (functional, allocated, or product baselines), to the extent that any of the following requirements would be outside specified limits or specified tolerances: safety, performance, reliability, maintainability, weight, balance, moment of inertia, interface characteristics, electromagnetic characteristics, and other technical requirements or specifications.

- b. Affects one or more of the following, after product baseline:
 - 1) Products furnished by the Government.
 - 2) Compatibility with interfacing products, including test equipment, support equipment, and associated software.
 - 3) Delivered operation or servicing instructions for which there are no planned and funded update requirements, such as for periodic or continual maintenance of instructions.
 - 4) Preset adjustments, to the extent that product identification should be changed.
 - 5) Interchangeability or substitutability of replaceable products, assemblies, or components.
 - 6) Change to a previously non-selected supplier, where supplier selection is specified.
 - 7) User skills or physical attributes.
 - 8) Operator or maintenance training.
- c. Requires retrofit of delivered products, by product recall, modification kit installation, or attrition (replacement during maintenance by modified spares).
- d. Affects cost or price to Government (including incentives and fees), guarantees, warranties, contracted deliveries or milestones, and is an engineering change that does not impact factors 1) through 3).

A Class I change shall require MDA approval IAW MDA Manual 3500.01-M.

3.10.4.1.2 Class II Engineering Change

The contractor shall classify a requested change as Class II when any engineering change does not impact any characteristics that would cause it to be classified as Class I.

A Class II change shall require Government involvement under these circumstances:

- a. The product baseline is established.
- b. The Government controls the product's detail design, its performance and interface attributes, and has imposed Government management procedures on the detail design.
- c. The contractual agreement stipulates either the cognizant MDA Program Office or designated representative(s) must review the change for classification, or must approve Class II changes.

3.10.4.2 Documenting Requests for Engineering Changes

The contractor shall clearly document engineering change requests and describe even slight changes so an audit trail can be constructed.

- a. Documentation for Class I engineering changes shall include:
 - 1) Unique change identifier.
 - 2) Originator organization and responsible individual.
 - 3) Class of change.

- 4) Product(s), major components, and interfacing products affected.
 - 5) Contract and configuration documents affected.
 - 6) Scope and description of change.
 - 7) Effects on specified performance, operation, maintenance, servicing, operation and maintenance training, spare and repair parts, and support and test equipment.
 - 8) Reason and justification for the change; and consequences of not doing the change.
 - 9) Priority/urgency of the change.
 - 10) Proposed change effectivity.
 - 11) Requested approval date.
 - 12) Change implementation and delivery schedules.
 - 13) Estimated cost increase or savings.
 - 14) Alternatives to the change.
- b. Documentation for Class II engineering changes shall include:
- 1) Unique change identifier.
 - 2) Originator organization and responsible individual.
 - 3) Class of change.
 - 4) Product(s), assemblies, and components affected.
 - 5) Configuration documents affected.
 - 6) Description of change.
 - 7) Reason for the change.
 - 8) Proposed change effectivity.

3.10.4.3 Configuration Control Board

The contractor shall establish a Configuration Control Board (CCB) with authority for achieving coordination necessary to evaluate a change and assess its impact to all stakeholders. The contractor's CCB shall:

- a. Be chaired by someone with authority to commit resources to implement the change.
- b. Include members that represent functional activities (e.g., Engineering, Quality, Safety, Maintenance, and Operations) and include technical Government representation.
- c. Provide review agendas and documents to board members before the meeting.
- d. Document, disseminate, and retain as record, board direction and decisions to all affected activities.

- e. Assure changes are necessary and consequences are acceptable.
- f. Assure changes have been properly identified, documented, reviewed, assessed, and classified.
- g. Assure planning for the implementation of the change into documents, hardware, software, and firmware is satisfactory.

The CCB shall disposition changes within its defined limited authority or to the portion of the "system" under its cognizance. Those changes that exceed the change approval authority of the CCB shall be elevated to a higher level.

The CCB agendas, documents, minutes, and decisions shall be stored in IDE ([3.1.5](#)).

The Government and contractor shall support MDA Program Change Board (PCB) activities.

3.10.4.4 Change Effectivity Determination

The contractor shall ensure change documentation delineates which unit(s) of the product are to be changed. Change effectivity shall include, as applicable, fabrication break-in and retrofit or recall.

A changed product shall not be distributed until required support and service areas are able to support it.

When determining the effectivity of a change, the contractor shall consider:

- a. Urgency of the change.
- b. Parts and materials on hand.
- c. Need to support multiple configurations when all existing units of the product will not be updated, or will not be updated at the same time.
- d. Timing of the introduction of the changed product, with respect to Government preferences and needs.

3.10.4.5 Change Implementation and Verification

The contractor shall implement an approved change IAW documented direction approved by the appropriate level of authority.

Implementation of a change shall include identification and release of new or revised configuration documentation, including requirements, design, and maintenance information. The release process shall correlate document revisions to change(s) incorporated. Document change notices that establish a permanent record of specific changes shall be used in disseminating document changes. For changes affecting interface, an Interface Change Notice (ICN) shall be generated and submitted to the appropriate CCB.

The contractor shall verify implementation of a change to ensure consistency among the product, its documentation, and its support elements.

The contractor shall perform verification of change implementation in the first affected unit to ensure consistency among the product, its documentation, and its support elements. Depending on the nature of the product and the complexity of the change, verification shall involve a detailed audit of the product against its documentation, a validation of operation, maintenance, installation, or modification instructions, or a simple inspection.

When the change is being introduced into a production line, the contractor shall ensure manufacturing instructions contain the change, are released for use, and first articles produced are inspected for compliance. The contractor shall develop a change implementation plan if support elements are impacted by the change, or the change is being retrofitted over time to a large number of units. The plan shall define the extent to which the change to each unit or support commodity is to be verified, and the records to be maintained. If the total quantity of materials, parts, or kits, is ordered in incremental stages, the contractor shall verify incremental ordering and supply operations are being completed.

3.10.4.6 Change Management Process Applied to Variances

The contractor shall document variances (waiver or deviation) when temporarily departing from baseline requirements. The appropriate authority shall approve all variances.

Products that incorporate a known departure from baseline requirements shall not be delivered to the Government unless a variance has been documented and approved. Variances are temporary departures from requirements and do not constitute a change to the configuration documentation. If the departure will be permanent, an engineering change is required. If variances impact operation, support, or maintenance; or impact the entire remaining number of deliverable units of the product, then an engineering change shall be proposed.

Requests for a variance shall include:

- a. Unique identifier for the variance.
- b. Originator organization and responsible individual.
- c. Classification of variance.
- d. Identifiers of the product(s) and components affected.
- e. Description of the variance, including any impacts to performance, servicing, quality, safety, training, spare and repair parts, and support and test equipment.
- f. Reason/justification for the variance.
- g. Priority/Urgency.
- h. Proposed effectivity of the variance (limited quantity or time).
- i. Corrective action to prevent recurrence and to eliminate the variance.
- j. Consideration for accepting variant products.
- k. Alternatives to variances.

3.10.4.6.1 Requests for Waiver

The contractor shall process a request for waiver if, during or after fabrication or maintenance of an item, which incorporates a known departure from requirements, it is determined the item is considered suitable for use-as-is or repairable by a nonstandard method. Requests for waivers shall be stored in IDE [\(3.1.5\)](#).

3.10.4.6.2 Requests for Deviation

The contractor shall process a request for deviation before fabrication of the item, if it is considered necessary to temporarily depart from mandatory requirements of the specification or drawings. Requests for deviations shall be stored in IDE [\(3.1.5\)](#).

3.10.4.6.2.1 Restrictions on Waivers and Deviations

- a. Effectivity. The effectivity of the request for waiver shall not include unprocessed units still deliverable under contract. For that case, an engineering change or deviation shall be submitted. The effectivity for the request for deviation shall be either the minimum number of units to support Engineering Change Proposal (ECP) generation and approval or the minimum number of units necessary to support return to the approved baseline configuration.
- b. Recurring. The contractor shall identify and minimize recurring waivers or deviations. A recurring waiver or deviation is a repeat or extension of a previously approved waiver or deviation. If it is necessary to request a waiver or deviation for the same situation, an engineering change shall be submitted.
- c. Software and Firmware. Waivers or deviations for software or firmware code listings shall not be submitted.

3.10.4.6.2.2 Classification of Waivers and Deviations

Each request for waiver or deviation shall be designated as critical, major, or minor by the contractor.

- a. Critical. A waiver or deviation shall be designated as critical when:
 - 1) The waiver or deviation involves safety.
 - 2) The waiver or deviation impacts a product characteristic classified as critical ([3.2.15.1](#)).
- b. Major. A waiver or deviation shall be designated as major when:
 - 1) The waiver or deviation impacts contract or configuration documentation requirements involving occupational health, performance, interchangeability, reliability, survivability, or maintainability of the item or its repair parts, effective use or operation, weight and size, or appearance (when a factor).
 - 2) The waiver or deviation impacts a product characteristic classified as major ([3.2.15.1](#)).
- c. Minor. A waiver or deviation shall be designated as minor when:
 - 1) The waiver or deviation does not involve any critical or major factors listed above.
 - 2) The waiver or deviation impacts a product characteristic classified as minor ([3.2.15.1](#)).

The contractor shall obtain concurrence on classification from the designated Government representative(s). Classification disagreements shall be referred to the cognizant MDA Program Office for decision by the Government representative(s). The cognizant MDA Program Office shall notify MDA/QS about any disagreement involving classification of a potentially critical waiver or deviation.

3.10.4.6.3 Review and Approval of Waivers and Deviations

Unless otherwise specified by the cognizant Government procuring activity, minor variances will be dispositioned by the cognizant Defense Contract Management Administration. Waivers or deviations classified as major shall be reviewed and approved by the cognizant MDA Program Office or specifically designated representative(s). Waivers or deviations classified as critical shall be reviewed and approved by MDA/DE, MDA/QS, and the cognizant MDA Program Office. Critical waivers or deviations which impact safety shall be assessed IAW [3.14.1.2.4](#).

3.10.5 Configuration Status Accounting

The contractor shall establish and maintain a Configuration Status Accounting (CSA) system, which correlates, stores, maintains, and provides, throughout the product's life, ready access to information about the product and its documentation. The CSA system shall consist of an information system capable of providing storage and security of product information and traceability of product history. The system shall provide structured records on the product and its related documentation. The system shall provide real time access and transfer of CSA information among customers, product development teams, and suppliers. The CSA system shall:

- a. Identify current approved configuration documentation (e.g., specifications, engineering drawings, software design documents, software code, procedures, and test plans) and identification number associated with each CI.
- b. Record and report status of proposed engineering changes and variances from initiation to final approval/contractual implementation.
- c. Record and report results of configuration audits to include status and final disposition of identified discrepancies.
- d. Record the "As-Designed", "As-Built", and "As-Maintained" configurations and changes, including status of waivers and deviations, and authorized substitutions and repairs (i.e., factory, fielded, or deployed), which affect configuration of a CI.
- e. Record and report implementation status, and verification of authorized changes, including product information change requests and change notices.
- f. Provide traceability of all changes from original baselined configuration documentation of each CI.
- g. Report effectivity, installation, and maintenance status of configuration changes and alterations to all CIs throughout the life cycle at all locations.
- h. Provide correlation between configuration status of software ([3.3.3.11.5](#)) and associated hardware and documentation.
- i. Provide for collection and reporting of a CI's complete configuration pedigree, including nonconformances ([3.10.3.1](#), [3.1.7](#)).
- j. Provide superseded configuration records that reflect previous product configurations.
- k. Provide records including customers and dates of delivery, installation configuration, service agreements, and warranties.
- l. Provide records on restrictions due to facility or product performance degradation.
- m. Provide relationships of data files, document representations, and key data elements to ensure data can be accessed or retrieved in a controlled manner.

The contractor shall review and analyze CSA data to detect and correct adverse trends. When potential or actual problems or delinquencies that impact MDA are detected, the contractor shall contact the cognizant MDA Program Office within one business day to establish a course of action to rectify the situation.

The contractor's CSA system shall have capability to access complete configuration information (i.e., configuration pedigree) on a product, any individual product unit, or group of product units. All CSA reports shall be stored in IDE ([3.1.5](#)).

3.10.6 Configuration Audit

The Government and contractor shall perform configuration audits (FCA (3.4.1.11) and PCA (3.4.1.13)) to establish performance and functional requirements defined in configuration documentation are achieved by the design and the design has been accurately documented. Configuration audits may result in audit findings, conclusions, recommendations, and action items. The audits remain open until all audit findings are closed and action items are completed. The contractor shall conduct configuration audits of supplier safety and mission critical items. Audit results shall be stored in IDE (3.1.5).

3.10.7 Configuration Management of Digital Data

The contractor shall establish a system for data configuration management, which assures integrity of digital data by providing:

- a. Effective file and database management.
- b. Unique identification.
- c. Retention of file and version relationships.
- d. Status of data.
- e. Controlled access to digital data.

3.10.7.1 Digital Data Identification

The contractor shall identify digital data files to differentiate between similar files and to maintain traceability to specific product configurations and representations. The contractor shall establish and apply these digital data identification rules:

- a. Assign a unique identifier to each file.
- b. Assign a unique identifier to each document representation.
- c. Assign a version identifier to each file.
- d. Maintain, in a data file, the relationship between:
 - 1) Document identifier and its revision level.
 - 2) Associated document representation(s).
 - 3) File identifiers and versions.
- e. Retain multiple versions of files with which to recreate prior document revisions and provide a traceable history of each document.

3.10.7.2 Data Status Level Management

The contractor's data status level management shall define and apply business rules based on status of a digital data document. Data status levels include definition, working, released, submitted, approved, and change to digital documents.

3.10.7.3 Digital Data Transmittal

When data is provided on media, appropriate identification, similar to software media identification, shall be affixed to media to clearly identify its contents. When it is impractical to include all file identifications, a reference to an accompanying listing or to a readme.txt file is required.

The contractor shall ensure deliverable digital data product can be recreated in readable form and processed by the user.

3.10.7.4 Data Access Control

The contractor shall employ an electronic data access process, which establishes access privileges to limit access to applicable users. Access privileges shall vary according to data status level, nature of the data, and user needs.

3.11 Control of Nonconforming Items and Materials

The contractor shall have a Nonconforming Items and Materials system that is compliant with the minimum requirements of SAE AS9100, Quality Management System – Requirements for Aviation, Space, and Defense Organizations, and is supplemented by these requirements. For new and existing systems, the contractor shall ensure:

- a. Items or material found to depart from drawings, specifications, or other requirements are conspicuously identified as nonconforming, segregated from conforming items or materials when feasible, and retained in a hold status until officially dispositioned and corrected.
- b. Effective corrective action is documented, implemented, and verified to prevent recurrence. All specified tests and inspections impacted by subsequent repair or rework processes shall be repeated.
- c. Nonconforming items are subjected to a nonconformance review process, which consists of a preliminary review and a Material Review Board (MRB). The MRB authority is authorized only at the prime contractor level IAW [3.11.2](#).

When nonconforming items or materials are detected after delivery to the customer, or use has started, the contractor shall notify the cognizant MDA Program Office and MDA/QS of the issue, including a description of its effects, potential effects, and any recommended corrective and preventive actions.

3.11.1 Preliminary Review

The contractor's preliminary review process shall be initiated with identification and documentation of a nonconformance. The preliminary review process shall be performed by authorized personnel to ensure nonconformances are properly documented and that appropriate examination and analysis of nonconformances are performed to determine cause, implement corrective and preventive action, and specify disposition. The preliminary review shall result in one of these dispositions:

- a. Remove from Use (Scrap). Items or materials that are unfit for use and are not economically repairable shall be processed IAW approved procedures for identifying, controlling, and disposing of unusable material.
- b. Return for Rework. Contractor manufactured items or materials, which are found to be incomplete or which can be corrected to completely conform to drawings, specifications, or other applicable requirements may be released for correction or completion of the remaining operations.
- c. Return to Supplier. Nonconforming items or materials received from a supplier may be returned for rework or replacement. The contractor shall provide the supplier with nonconformance information and applicable instructions for re-submittal of corrected material and associated corrective action reports.
- d. Standard Repair. Contractor personnel performing preliminary review may authorize repair using the cognizant MDA Program Office approved standard repair procedures included in the item's configuration documentation. Minor repairs made via approved standard repair procedures do not require a waiver to be processed. Contractor shall track use of standard repairs per product and report the data to the cognizant MDA Program Office. More than one standard repair on the same safety or mission critical item shall require a waiver request processed IAW [3.10.4.6](#).
- e. Submit to MRB. If none of the above dispositions are appropriate, the item or material shall be submitted for MRB action.

3.11.2 Material Review Board

Material Review Board dispositions shall be authorized only at the prime contractor level. Authority from the prime contractor to allow any subcontractor or supplier to disposition nonconforming items and material shall not be permitted. To maintain visibility and ensure effective corrective action is maintained throughout the supply chain, all dispositions shall be maintained and approved at the prime contractor level.

3.11.2.1 Material Review Board Membership

The prime contractor's MRB shall consist of a core team of personnel who have authority and responsibility for assuring MRB actions are performed in compliance with requirements of this provision. The MRB core team shall have representation from engineering and quality disciplines and a designated Government representative. The designated Government representative shall be a voting member of the board and appointed by the cognizant MDA Program Office with concurrence from the Quality, Safety, and Mission Assurance Directorate (MDA/QS). All MRB members shall be selected on the basis of their technical competence.

3.11.2.2 Material Review Board Dispositions

In determining disposition of nonconforming items, the MRB shall consider the effect of nonconformance upon intended use and review any records of MRB actions on similar items. The MRB review findings, recommendations, and disposition actions, shall be documented and stored in IDE (3.1.5). The MRB actions are subject to review by the cognizant MDA Program Office or designated representative. The MRB may make preliminary review dispositions. The MRB may also recommend the following dispositions:

- a. Nonstandard Repair. If repair to an acceptable condition is considered possible and desirable, but a standard repair procedure approved by the cognizant MDA Program Office is not applicable, a waiver request shall be processed IAW [3.10.4.6.1](#)
- b. Use-As-Is. If the nonconforming item is considered usable as is, a waiver request shall be processed IAW [3.10.4.6.1](#).

Waiver requests for repair or Use-As-Is dispositions shall be reviewed and approved IAW [3.10.4.6.3](#). Approval or acceptance of nonconforming items and material is the sole prerogative of the Contracting Officer. The contractor shall maintain metrics of MRB actions and dispositions and report IAW Appendix B, [B.4.7.16](#).

3.12 Fabrication and Quality

The contractor shall establish and maintain control systems for operations associated with fabrication and quality, including any related measurement and analysis, which support the fabrication process and ensure specification requirements are achieved, verified, and maintained. Fabrication and quality activities shall be planned, implemented, and controlled to provide for an efficient and effective program. Established techniques for monitoring fabrication processes shall be used to ensure process capabilities remain adequate to produce required product characteristics. Product conformance shall be verified using quality verification techniques. Process and quality records generated during the fabrication process shall be stored in IDE [\(3.1.5\)](#).

The contractor shall have a fabrication and quality process that is compliant with the minimum requirements of SAE AS9100, Quality Management System – Requirements for Aviation, Space and Defense Organizations. Some assurance related activities not covered by SAE AS9100 requirements are identified in the following sections and supplement SAE AS9100 requirements.

3.12.1 Manufacturing, Process, and Quality Control Planning

The contractor shall plan the necessary process and quality controls, including any related measurement and analysis, to be used throughout fabrication. The contractor shall prepare a manufacturing plan that shall:

- a. Establish levels, depth, and extent of process control, test, and inspection to be implemented based upon product and process specification requirements, classification of characteristics, and integrated test program results.
- b. Use process flow diagrams, or equivalent, to identify processes, including critical and key characteristics, relating to fabrication, inspection, and test.
- c. Identify requirements for materials, test equipment, tooling, equipment, personnel skills, facilities, and related software and its maintenance.
- d. Identify any packaging, handling, transportation, and storage requirements from receiving through delivery.

The manufacturing plan shall be stored in IDE [\(3.1.5\)](#).

3.12.2 Process Selection and Development

The contractor shall establish and maintain a system for selection and development of fabrication processes concurrent with evolutionary design of the product. The contractor shall analyze the ability of proposed processes to fabricate quality hardware with minimum variability, using design for producibility methods and continuous process improvement.

3.12.2.1 Process Selection and Development Planning

The contractor shall perform process selection and develop planning to support fabrication efforts. Planning shall reflect a phased process maturity approach to support evolutionary acquisition, including transitioning to mature production processes [\(3.2.18\)](#). As a minimum, planning shall address:

- a. Criteria and methods used to determine appropriate control of processes throughout development, such as process capability, inspectability, scrap and rework costs, and the required level of quality and reliability.
- b. Criteria and methods for determining the stage of development (e.g., prototype, engineering model, and production), characterization, capability demonstration, and process qualification to be performed throughout development.

- c. Criteria and methods for determining which processes shall be controlled by specifications. Criteria shall be based upon tolerances, criticality, and application of the product, contractor experience with the process, process complexity, required operator skill level, inspectability, and the extent of subsequent test and inspection.
- d. Criteria and methods for determining and controlling mission critical processes whose failure can significantly affect system safety, mission success, availability, or total maintenance/logistics support costs.
- e. Criteria and methods for determining special processes for which resulting output cannot be readily or economically verified by subsequent monitoring or measurement, or where test or inspection methods would result in destruction of the finished item.

3.12.2.2 Mission Critical Process Selection

The contractor shall identify mission critical processes based on any one, or appropriate combination of:

- a. Outputs from Reliability Analyses ([3.5.6](#)); Failure Modes, Effects, and Criticality Analysis (FMECA) ([3.5.6.1](#)); and Process Failure Modes Effects Analysis (PFMEA) ([3.5.14](#)).
- b. Application of advanced state-of-the-art techniques.
- c. Complex productivity or technical complexity.
- d. Proprietary design.
- e. Limited source, limited material, or sole source availability.
- f. Past experience and judgment on similar processes warrants the process be identified as critical.
- g. Physical properties of the item are stability sensitive, requiring tight process control.

3.12.2.3 Special Processes

The contractor shall identify and control special processes used to support fabrication of the item, as required by SAE AS9100. The contractor shall certify personnel performing special processes (e.g., nondestructive testing, welding, and soldering) using requirements specified in the associated military or industry process standard and IAW [3.1.9.2](#). The contractor shall certify and maintain special process tools and equipment, which assures quality of the end product.

3.12.3 Product Test and Inspection Plan

The contractor shall establish and maintain Product Test and Inspection Plan(s) (PTIP) to indicate tests and inspections to be conducted during all phases of fabrication, from source or receiving, through final acceptance. Fabrication points at which tests and inspections are to be made shall be specifically identified in fabrication flow documentation (e.g., travelers or operations sheets). Sufficient examination points shall be specified to ensure tests and inspections are conducted before work operations that will preclude detection and correction of deficiencies or result in excessive rework, repair, or cost. The extent of test or inspection shall be consistent with criticality of the characteristic. The PTIPs shall be stored in IDE ([3.1.5](#)). The PTIP shall include:

- a. Flow diagrams, or equivalent, indicating sequence of production operations showing tests, inspections, and process control points.
- b. Reference to procedures used for acceptance test and inspection.

- c. Identification of the part or identifying number and name for each item.
- d. Identification of items requiring environmental stress screening ([3.5.13](#)), burn-in tests, production assessment testing, and any other special tests.

3.12.4 Fabrication and Quality Procedures

The contractor shall establish and maintain a system to develop and control fabrication, test and inspection procedures, and workmanship standards ([3.12.4.3](#) and [Appendix C](#)). Procedures and workmanship standards shall be readily available in the manufacturing, test, and inspection areas.

3.12.4.1 Fabrication and Process Procedures

The contractor shall establish and maintain procedures for fabrication, processing, assembly, rework, repair, packaging, handling, transportation, and storage operations, as required by SAE AS9100. Additionally, these procedures shall contain or reference:

- a. Required workmanship standards and production aids, visual aids, including material and process specifications and standards applicable to each process.
- b. Step-by-step instructions for performing operations and methods for recording completion of each operation.
- c. Identification of equipment, tools, and software required, including requirements and methods for certifying tools, equipment, and associated software.
- d. Special conditions required to be maintained, such as conditions required for parts, devices, and material protection, environmental conditions, safety controls, and equipment maintenance.
- e. Required characteristics and tolerances, including identification of particular process variables to be controlled, and methods by which variables will be monitored.
- f. Identification of mandatory contractor and Government inspection points ([3.1.12.2](#)).
- g. Requirements for recording process data, data analyses to be performed, and responsibilities and actions assigned to ensure control of the process.
- h. Identification of any special handling devices required for movement of parts, devices, and material.
- i. Identification of applicable required personnel certification(s) and training.

3.12.4.2 Test and Inspection Procedures

The contractor shall prepare procedures for tests and inspections, in compliance with SAE AS9100. Additionally, procedures shall include or reference:

- a. Tolerances, levels, or limits of inputs for the characteristics being tested or inspected.
- b. Identification and setup of test and inspection equipment and related software.
- c. Environmental stress levels required during test or inspections.
- d. Method of performing the test or inspection, including sequential steps.
- e. Special pretest and inspection instructions.
- f. Acceptance and rejection criteria.

- g. Required safety precautions.
- h. Applicable personnel qualification or certifications required.

Acceptance test and inspection procedures used as a basis for Government acceptance of contract end items shall be submitted into IDE ([3.1.5](#)) and marked for approval by the cognizant MDA Program Office. Notification that acceptance test and inspection procedures are submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.12.4.3 Workmanship Standards

The contractor shall use approved workmanship standards. Workmanship standards shall be referenced in fabrication, test, and inspection procedures, and shall be readily available in the production, test, and inspection areas. The contractor may propose alternate workmanship standards for MDA/QS approval. Proposed workmanship standards shall be accompanied by objective data documenting that mission safety or reliability will not be compromised. These following MDA/QS recognized workmanship standards shall be used:

- a. Requirements for Soldered Electrical and Electronic Assemblies (IPC J-STD-001, Class 3).
- b. Space Applications Electronic Hardware Addendum to IPC J-STD-001, Class 3, Requirements for Soldered Electrical and Electronic Assemblies (IPC J-STD-001ES).
- c. Requirements and Acceptance for Cable and Wire Harness Assemblies (IPC/WHMA-A-620, Class 3) including Amendment 1.
- d. Space Applications Electronic Hardware Addendum to IPC/WHMA-A-620 (IPC/WHMA-A-620B-S).
- e. Fiber Optics Terminations, Cable Assemblies, and Installation (NASA-STD-8739.5).
- f. ESD Control Program (MIL-STD-1686 or ANSI/ESD-S20.20-2007).
- g. Printed Board Design (IPC-2220 Series, Class 3).
- h. Printed Board Manufacturing (IPC-6010 Series, Class 3).
- i. Qualification and Performance Specification for Rigid Printed Boards (IPC-6012, Class 3/A).

Mechanical design and workmanship standards are specified in MDA-QS-003-PMAP.

3.12.4.3.1 Connector Mating and Demating

The contractor shall establish and maintain approved connector mating and demating procedures that adhere to practices and specified requirements cited in Appendix C Workmanship Requirements. The contractor's procedures shall be traceable to a military specification or an industry standard and include requirements for training and qualification. The contractor should consider NASA-STD-8739.4 Crimping, Interconnecting Cables, Harnesses, and Wiring as guidance for connector mating and demating.

3.12.4.3.2 Threaded Fasteners and Torque

The contractor shall establish and maintain approved threaded fastener and torque procedures that adhere to practices and specified requirements cited in Appendix C Workmanship Requirements. The contractor's procedures shall be traceable to a military specification or an industry standard and include requirements for training and qualification. The contractor should consider NASA-STD-5020 Requirements for Threaded Fastening Systems in Spaceflight Hardware as guidance for threaded fastening systems.

3.12.5 Product Control during Fabrication

The contractor shall establish and maintain a system for control of parts, devices, and materials used throughout the fabrication process, as required by SAE AS9100, MDA-QS-003-PMAP; and as supplemented in the following paragraphs.

3.12.5.1 Product Identification and Handling

The contractor shall establish and maintain a process for identification and handling of parts, devices, and materials during fabrication. Controls shall ensure:

- a. Only authorized parts, devices, and materials that meet specified requirements are released to manufacturing operations.
- b. Parts, devices, and materials excess to manufacturing operations are removed from the processing area and reviewed to determine need for re-inspection before returning to their respective stock points.
- c. Parts, devices, and materials procured for development are not installed in production end items without approval from the cognizant MDA Program Office.
- d. Hardware items used as aids or tools are conspicuously marked to prevent installation in end items.
- e. Deliverable hardware shall not be used as test, production, or troubleshooting aids.
- f. Parts, devices, and materials sensitive to electrostatic discharge shall be identified and appropriate precautions incorporated into storage, handling, fabrication, and test operations.

3.12.5.2 Product Protection

As a supplement to the SAE AS9100 requirements, the contractor shall establish and maintain controls to assure quality and reliability of the product. Parts, devices, and materials subject to damage, deterioration, electrostatic discharge, contamination, or foreign object debris shall be identified and protected throughout fabrication. Personnel working on MDA hardware shall use appropriate safeguards when handling hardware. Additionally, implementing procedures for parts, devices, and material protection shall, as a minimum, comply with specified material protection requirements for environment, cleanliness, contamination control, and foreign object elimination.

3.12.5.2.1 Electrostatic Discharge Controls

For electronics, the contractor shall establish and maintain an electrostatic discharge (ESD) control program IAW MIL-STD-1686 or ANSI/ESD-S20.20. As a minimum, the ESD control program shall address training ([3.1.9.1](#)), protected work area procedures and verification schedules, packaging, facility maintenance, storage, and shipping. As a supplement to the MIL-STD-1686 and ANSI/ESD-S20.20 requirements, relative humidity (RH) shall be controlled from 30% to 70% and ionizers used when the RH falls below 40%, with no device or circuit card handling allowed if the humidity falls below 25%. Alternative limits may be proposed to MDA Parts, Materials, and Process Board for approval (MDA-QS-003-PMAP, paragraph 2.1).

Unrestricted airflow between ionizer and the ESD sensitive (ESDS) item is required. For storage of ESDS devices, the relative humidity shall be maintained between 25% and 75%.

A check of the RH level in each ESDS area shall be performed at the start of the workday and the result shall be logged. Periodic observations of the RH level should be made to ensure continual compliance.

The records of continual RH monitoring (chart recorders or data loggers) shall be retained as required by contract.

For static sensitive ordnance, the contractor shall establish and maintain an ESD program. Personnel and equipment in hazardous locations and locations where static sensitive ordnance are exposed shall be grounded in a manner that discharges static electricity and prevents static electricity accumulations that may be capable of initiating dusts, gases, vapors, or exposed ordnance. Permanent equipment shall be bonded to the facility grounding system. Additionally, static sensitive ordnance operations shall not be conducted when the relative humidity is less than 35%. Where humidity requirements cannot be met, a static charge risk assessment shall be performed to identify and mitigate potential ESD risks.

The contractor shall establish and maintain an ESD Control Plan that describes planning and implementation of ESD Controls for both electronics and ordnance. The ESD Control Plan shall be stored in IDE [\(3.1.5\)](#).

3.12.5.2.2 Contamination Control Program

The contractor shall establish and maintain a Contamination Control Program (CCP) appropriate for hardware. Contamination includes all materials of molecular and particulate nature whose presence degrades hardware performance. The program shall include a contamination control verification process, which considers the hardware's contamination sensitivity and allowance. The verification process along with the specific cleanliness requirements and approaches to be followed shall be documented in a CCP and stored in IDE [\(3.1.5\)](#).

The CCP shall describe methods used to measure and maintain levels of cleanliness required throughout the item's life. Contamination control of hardware shall be compatible with the most contamination sensitive components. The CCP shall include data on material properties, design features, test data, system tolerance of degraded performance, and methods to prevent degradation and allow for evaluation of contamination hazards.

3.12.5.2.2.1 Clean Rooms

When handling contamination sensitive hardware, the contractor shall implement clean room standards appropriate to product application and complexity. The contamination potential of material and equipment used in cleaning, handling, packaging, tent enclosures, shipping containers, bagging (e.g., anti-static film materials), and purging shall be described in detail for each subsystem or component at assembly, integration, and test.

3.12.5.2.3 Foreign Object Elimination Program

The contractor shall establish and maintain a Foreign Object Elimination (FOE) program, which systematically eliminates Foreign Object Damage and Debris to preserve safety, quality, and reliability. National Aerospace Standard NAS 412 shall be used as a guideline. The FOE program shall provide for a standardized approach that maintains awareness, prevention, and compliance; and assures continued reinforcement. The FOE program shall also ensure operational processing areas maintain a safe, clean, and Foreign Object Debris Free environment, with appropriate controls commensurate to the criticality of the hardware, including requirements for current FOE Metrics, tool control, hardware accountability, personal items, and consumables control. The contractor shall develop and maintain FOE Program Plan(s) that specifies requirements, techniques, and training for implementing and assuring effective FOE awareness and prevention throughout the supply chain. The FOE Program Plan shall be stored in IDE [\(3.1.5\)](#).

3.12.5.3 Product Status Indication

The contractor shall establish and maintain a system for product status indication that assures:

- a. The inspection and test status of parts, devices, materials, and assemblies are clearly indicated throughout the entire fabrication cycle. Records indicating completion of all tests, inspections, and

operations, which reference all discrepancy reports, shall be readily available in the area where the item is located, and stored in IDE [\(3.1.5\)](#).

- b. Only authorized personnel shall designate parts, devices, materials, or assemblies as acceptable. Records documenting each designation shall also provide traceability to the individual making the designation.
- c. Stamps or other status indicators shall be of a design distinctly different from those used by the Government.

3.12.6 Fabrication Process Control

In addition to SAE AS9100, the contractor shall control fabrication processes IAW specified operating procedures. Process data shall be recorded and analyzed to ensure continued process control. The contractor shall record process variables data necessary for analysis to determine trends and to maintain continued process integrity and control. Specific controls shall be consistent with:

- a. The product characteristics and their associated tolerances, criticalities, sensitivity to process variation, inspectability, and testability.
- b. The application and operational requirements of the product.
- c. The extent and nature of subsequent test and inspection.
- d. Operator skill required.
- e. The results of process selection and development.

When a process does not meet either specification or process control limits, the possible effect on items previously processed shall be determined and corrective action taken to ensure items processed meet specification requirements or are identified as nonconforming [\(3.11\)](#).

3.12.6.1 Process Qualification and Requalification Program

The contractor shall implement a process qualification program to prove-in new or modified (e.g., material and process changes, technology insertion, or redesign) fabrication processes and test. Process qualification shall be performed using tools and equipment, software, personnel, material, and procedures used to fabricate and ensure product quality. During process qualification, the contractor shall identify and resolve potential fabrication process and product failure modes using PFMEA [\(3.5.14\)](#) to improve quality and reliability of the product. The contractor shall requalify processes whenever a change occurs, that may adversely affect the product. Process requalification is required for material and process changes; tooling, dies, or fixture changes; equipment, procedure, or software changes; fabrication rate changes; relocation; and breaks in fabrication of greater than 12 months. The PMPCB (MDA-QS-003-PMAP, paragraph 2.2) shall approve process qualification and requalification. The contractor shall notify the cognizant MDA Program Office, and designated representative(s) of process qualification and requalification events to allow for participation. Process qualification and requalification events shall be documented and stored in IDE [\(3.1.5\)](#).

3.12.6.2 Fabrication and Quality Metrics

The contractor shall establish and maintain a process for collection and analysis of fabrication and quality metrics. As a minimum, the set of metrics and frequency of collection should be representative of the development effort and phase of the acquisition process.

3.12.6.3 Fabrication Defects

The contractor shall detect, document, and correct (3.1.10) defects during fabrication and assess potential process improvement opportunities. When required, the contractor shall conduct analysis to determine defect root cause and take action to prevent recurrence. Data on defects, as identified in inspections, document reviews, and testing, shall be collected and analyzed by the contractor. Defects shall not be reprocessed until they have been documented and dispositioned. The contractor shall provide feedback on status and results of defect preventive and corrective action to project personnel on a periodic basis.

3.12.6.4 Continuous Process Improvement

The contractor shall determine key product characteristics and process parameters suitable for process control and monitor them using metrics. Process operations, parameters, and characteristics shall be determined on the basis of criticality, cost effectiveness, and technical considerations and included in the Transition to Production Plan (3.2.18.1). Continuous improvement program shall:

- a. Provide a focus for product improvement through identification of sources of variation and key characteristics.
- b. View the quality of a key characteristic as its conformance to nominal rather than merely achieving tolerance.
- c. Reduce the variation in key characteristics by improving consistency of measurement systems; identifying, eliminating, and controlling sources of variation; and controlling the process rather than the product.

3.12.7 Fabrication Environmental Stress Screening

During fabrication, the contractor shall implement the Environmental Stress Screening (ESS) program (3.5.15) to surface defects by stressing the item without degrading its inherent reliability. Environmental stresses may be applied in sequence or in combination, with the intent of stimulating hardware defects. The ESS program should not be used to simulate an operational environment. Results of ESS shall be used to continually improve manufacturing processes, and stored in IDE (3.1.5).

3.12.8 Fabrication Quality Verification

The contractor shall perform tests and inspections using documented procedures. Fabrication quality verifications, including in-process, acceptance, first article, and nondestructive tests and inspections, shall be performed to ensure conformance to product or process specifications. Personnel performing these verifications shall have the training, certification (3.1.9), and authority to report problems and failures without concern for the cost, schedule, or technical implications of the reported problem or failure. When items rejected during fabrication quality verification are returned for completion of missed operations, rework, or repair, fabrication quality verification shall be accomplished not only for that specific characteristic but also for other characteristics that may be affected.

3.12.8.1 In-Process and Acceptance Test and Inspection

The contractor shall perform in-process testing and inspection during fabrication to verify adequacy and control of operations. Tests and inspections used as a basis for Government acceptance of contract end items shall be performed IAW procedures approved by the cognizant MDA Program Office or designated representative(s). Test and Inspection Procedures shall be submitted into IDE (3.1.5) and marked for approval by the cognizant MDA Program Office. Notification that test and inspection procedures are submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. Tests and inspections shall:

- a. Be performed at, or before, the last point at which the acceptability of the item or characteristic may be completely verified.
- b. Provide a measure of product and process quality, which results in data suitable for analysis and timely correction of adverse quality trends.
- c. Be performed in a manner and under conditions that simulate product end use to the highest degree practicable.
- d. Be sufficient to provide assurance the product conforms to specification requirements.

3.12.8.2 First Article Test and Inspection

First article test and inspection shall be performed on safety and mission critical items ([3.5.7](#)) manufactured or purchased by the contractor. First article test and inspection shall be conducted before initiation of a production run and on the first items produced using new or modified tooling or processes. First article test and inspection shall consist of a comprehensive test and inspection to verify production capability; proper use of materials, parts, and process controls, to demonstrate product compliance to specified requirements; and to verify validity of applicable documentation. First article test and inspection results shall be stored in IDE ([3.1.5](#)).

3.12.8.3 Nondestructive Test and Inspection

The contractor's nondestructive tests and inspections shall be controlled by standards, specifications, and procedures; certification of personnel; and proper equipment controls. Nondestructive test and inspection results shall be stored in IDE ([3.1.5](#)).

3.12.8.4 Nonconforming Items Control

The contractor shall control, review, and disposition nonconforming parts, devices, and materials used during fabrication IAW SAE AS9100 and the requirements contained in [3.11](#).

3.12.9 Fabrication and Quality Records

The contractor shall maintain fabrication and quality records IAW SAE AS9100 and as supplemented in the following paragraphs. Additionally, fabrication and quality records shall be incorporated into the pedigree program ([3.1.7](#)). Fabrication and quality records shall be stored in IDE ([3.1.5](#)).

3.12.9.1 Fabrication Records

The contractor shall ensure fabrication data, including defects, are recorded and retained in sufficient detail to indicate accountability for operations, provide for analysis to determine problem frequency and trends, and implement appropriate preventive and corrective actions. Records shall be traceable to specific personnel or equipment where personnel skills or equipment capability have a significant effect on product quality. Before disposal of fabrication records, the contractor shall inform the cognizant MDA Program Office.

3.12.9.2 Quality Control Records

The contractor shall maintain records of tests and inspections performed. Records shall be appropriate for the type, scope, and importance of test or inspection performed and sufficiently detailed to provide objective evidence of conformance to requirements and to permit necessary analysis for further action. Records shall include inspection results, evidence of performance of required test or inspection, extent of nonconformance, disposition of nonconforming items, and responsibility for corrective action. Records for acceptance test and inspection shall include identification of specific equipment (e.g., model and serial number) used for acceptance, so that recall of accepted products may be accomplished when out-of-

tolerance conditions are noted during subsequent calibrations. Before disposal of quality control records, the contractor shall inform the cognizant MDA Program Office.

3.12.9.2.1 Closeout Photographs

The contractor shall capture closeout photographs of all safety and mission critical items, subsystems, and systems during build up, closeout operations, and before the last point at which the unit can be verified. Closeout photographs during manufacturing of Commercial-Off-The-Shelf (COTS) items are not required. Closeout photographs review shall be performed and completed by the responsible engineer or subject matter expert during build up inspection, and corrective action taken on any issues discovered, prior to initiating the next level of assembly or operation (e.g., build up, movement, or emplacement). Closeout photographs shall have enough detail to support final acceptance, failure analysis, parts and materials identification including legible lot number/date code, hardware workmanship, and configuration. The contractor shall provide closeout photograph review results to support customer acceptance and mission assurance review decisions. Closeout photographs shall be stored in IDE [\(3.1.5\)](#).

3.12.10 Packaging, Handling, Storage, and Transportation of Product

The contractor shall establish and maintain a system for packaging, handling, storage, and transportation of product. The system shall comply with product specifications and regulations and include documented procedures to prevent product degradation.

3.12.10.1 Packaging

The contractor shall perform preservation packaging, packing, and marking processes (including materials used) IAW the item specification and system requirements.

3.12.10.2 Handling and Storage

To prevent deterioration, the contractor shall establish and maintain processes and procedures for handling and storage of product. The handling and storage procedures shall be adhered to and identified on fabrication documentation. These criteria shall be used, as appropriate, for establishing handling and storage procedures for product:

- a. Control of environment (e.g., temperature, humidity, contamination, and pressure).
- b. Measures and facilities to segregate and protect product routed to different locations such as the materials review crib, a laboratory for inspection, or return to the manufacturer from unaccepted shipments.
- c. Easily identifiable containers, to identify product.
- d. Control measures to limit personnel access to product during receiving inspection and storage.
- e. Facilities for interim storage of product.
- f. Provisions for protective cushioning, as required, on storage area shelves and in storage and transportation containers.
- g. Protective features of transportation equipment designed to prevent product from being dropped or dislodged during transit.
- h. Protective bench surfaces on which product is handled during operations (e.g., test, assembly, inspection, and organizing kits).
- i. Required use of gloves, finger cots, or other means when handling product.

- j. Electrical, Electronic, and Electromechanical parts shall be kept in a temperature and humidity controlled environment to prevent moisture absorption. Plastic encapsulated devices are to be handled in such a way as to minimize moisture absorption and ionic contamination.
- k. Products sensitive to electrostatic discharge shall be identified and appropriate precautions incorporated into storage, handling, fabrication, test, and shipping operations.
- l. Unique product criteria.

3.12.10.3 Preparation for Shipment and Transportation

The contractor shall arrange for the protection of the quality of product after final inspection and test. Where contractually specified, product protection shall be extended to include delivery to destination.

Items shall be identified and packaged IAW contractual requirements and documented procedures. The contractor shall inspect and control items being prepared for shipment and transportation to ensure:

- a. Items have satisfactorily passed applicable inspections and tests.
- b. Items have been identified, preserved, packaged, and packed IAW applicable specifications and procedures.
- c. Packaging and containers have been marked IAW applicable drawings, specifications, and procedures.
- d. Environmental conditions of shipping containers are monitored during shipment, as appropriate.

The contractor shall ensure accompanying documents for the product are present at delivery, as specified in the contract or purchase order, and are protected against loss and deterioration.

3.12.11 Lifting Devices and Equipment Program

The contractor shall establish and maintain a Lifting Devices and Equipment Program for critical lifts of hardware. The Lifting Devices and Equipment Program shall include equipment and personnel involved in its management, operation, alteration, test, inspection, maintenance, certification, and acquisition. Weight handling equipment includes, cranes and hoists (e.g., fixed and mobile), rigging gear (e.g., slings and shackles), and associated equipment (e.g., chain falls and dynameters).

Lifting devices and equipment used for ordnance shall be properly grounded ([3.12.5.2.1](#)). Personnel involved in lifting operations shall be trained and certified ([3.1.9](#)).

When the contractor is performing critical lifts at test ranges, range requirements supersede this requirement.

3.12.11.1 Identification of Critical Lifts

The contractor shall establish and maintain criteria to identify critical lifting operations and lifting devices or equipment. Criteria shall be approved by the contractor's facility and safety organizations and stored in IDE ([3.1.5](#)).

3.12.11.2 Lifting Devices and Equipment Program Certification

Certification of contractor's lifting devices and equipment ([3.1.9.2](#)) shall be initially performed and then recertified on a periodic basis. Recertification shall consist of a review of all applicable maintenance records, condition inspection, and load test data, including traceability, to ensure handling equipment has been maintained in a safe and serviceable condition and is functioning properly. Minimum requirements

for managing lifting devices and equipment and establishing periodic test load, test frequency, and inspections, is contained in NASA-STD-8719.9. Alternate inspection, testing, and certification methods shall be approved by the cognizant MDA Program Office or designated representative(s).

3.12.11.3 Identification of Critical Moves

The contractor shall identify criteria for determining critical moves, and establish and maintain processes and procedures for movement or transport of critical hardware to prevent damage or loss. Critical moves shall be completed by authorized, trained, and qualified personnel. Additional trained and qualified personnel shall be utilized when moving critical hardware that cannot be safely moved by one individual.

3.13 Supplier Management

The Government and contractor shall establish and maintain a supplier management program to ensure selection of suppliers capable of attaining program cost, schedule, and technical objectives during development and production phases. The contractor's supplier management program shall comply with SAE AS9100 requirements and the following requirements. Requirements include appropriate flow down requirements such as program quality, MDA Assurance Provisions (MAP), MDA Parts, Materials, and Processes Mission Assurance Plan (PMAP), specifications, program unique terms and conditions, and any metrics to be communicated, tracked, and monitored during the planning and execution phase of the supplier management process. Throughout the acquisition process, the supplier management program shall be focused on providing effective and timely products and services.

3.13.1 Supplier Selection

The Government and contractor shall establish and maintain a process for evaluation and selection of procurement sources. The Government and contractor shall evaluate and select sources based on their technical capability and capacity to supply products (hardware, software, and services) with acceptable levels of quality and reliability, IAW program requirements. Contractor criteria for supplier selection, evaluation, and re-evaluation shall be established and include:

- a. Documented and implemented quality system that includes tracking of safety issues.
- b. Development, manufacturing, and verification capability.
- c. Software maturity, software engineering, software quality including safety, and software configuration management.
- d. Past performance/quality history and field data.
- e. Available personnel and resources.
- f. Source inspection, receiving inspection, and test results.
- g. On-time delivery performance.
- h. Corrective action responsiveness.
- i. Life cycle support processes.
- j. Financial and organizational stability.
- k. Fact finding visit results.

An onsite survey of supplier's capabilities, facilities, and technical management program shall be conducted by the contractor if no previous quality and reliability records are available, or if supplier performance has been marginal, based on supplier ratings. Results of this survey and subsequent corrective action shall be documented, maintained, and stored in IDE ([3.1.5](#)).

The contractor shall select suppliers based on overall best value in terms of performance, risk factors (e.g., reliability, technology, diminishing sources, counterfeit parts, and foreign influence or ownership), cost or price, and quality factors. The contractor shall use the requirements of MDA-QS-003-PMAP-REV B sections 3.6.7 Counterfeit Parts and Materials, and 3.7 PMP Procurement Management when selecting suppliers to reduce the risk of introducing counterfeit parts and materials into design and end item deliverables.

The performance of each supplier shall be objectively evaluated by the contractor on a continuing basis using data from source inspection, receiving inspection, qualification, fabrication, assembly, acceptance test and inspection, on-site surveys, audits, field use, engineering and qualification, alerts, and any other available quality data. The contractor shall periodically evaluate the supplier's financial and organizational stability and perform a study for qualifying other suppliers when necessary. Based on this evaluation, the contractor shall prepare, maintain, and use approved source lists, or equivalent, organized by supplier, facility location, and each product type or service, and its intended application. Criteria for maintenance of the approved source list, including addition and removal of suppliers, shall be documented. Records of selection, evaluation, and approval shall be maintained and stored in IDE (3.1.5). The contractor shall maintain rationale for their selection of sole source suppliers. The contractor shall consider cost effectiveness of qualifying multiple sources for critical components.

3.13.1.1 Safety and Mission Critical Supplier List

The contractor shall establish and maintain a safety (3.14.1.2.2) and mission critical (3.5.7) supplier list. This list shall be an input to the supplier management system (3.13.4.1). The list shall be stored in IDE (3.1.5).

3.13.1.2 Conditional Source Approval

The contractor shall establish and maintain a process for source approval for emergency or conditional procurement to be used in deliverable product. Procurements from sources other than those on approved source lists shall not be made without appropriate engineering and quality review and written approval from program management. If use of an unapproved supplier is necessary on a conditional basis, steps shall be promptly taken to approve the source. The system shall include a process for storage, identification, tracking, and traceability of supplies from unapproved sources. Until the supplier is approved, the system shall prevent product from being shipped or presented to the Government for acceptance. In the event the supplier fails to qualify, suitable corrective action shall be initiated, before any subsequent purchase. Receiving inspection or validation for software shall be performed to ensure items procured on a conditional basis conform to purchase order, specification, and drawing requirements. Satisfactory performance of supplies purchased from an unapproved supplier shall not constitute qualification of that supplier.

Purchases from unapproved sources may be made if material purchased is not included in deliverable product.

3.13.2 Supplier Ratings

The contractor shall establish and maintain a supplier rating system that uses a continual and standardized methodology for monitoring, evaluating, and improving supplier performance. The contractor shall monitor and control suppliers IAW their flow down requirements, including metrics, procedures, and planning. The supplier rating system shall define minimum acceptable rating criteria for hardware, software, and services. The rating system shall be based on quality, delivery performance factors, and other subfactors, such as post acceptance events and responsiveness to corrective action requests. Factory failures and field data shall directly affect a supplier's overall rating. Supplier monitoring results shall be used as a factor to determine supplier ratings. The system shall use a centralized repository that includes both historical and current data on supplier performance. Ratings shall be based on both recent and cumulative performance rather than solely on short term windows of reference. The contractor shall communicate ratings to their suppliers as part of the continual improvement process to enable suppliers to proactively self manage and improve performance. Departures from plans, procedures, or flow down requirements shall be reviewed with the contractor and corrective action taken as directed. A poor quality rating shall prohibit the placing of any purchase order without further investigation, satisfactory corrective action from the supplier, and approval from top-level management.

3.13.3 Supplier Evaluations

The contractor shall establish and maintain a system to schedule and conduct on-site supplier evaluations to ensure compliance with procurement document requirements. The frequency, scope, and method for evaluating shall be based upon criticality or complexity of items being procured, known problems or difficulties, documented risks, and quality history. The planned coverage of each evaluation shall be documented. Coverage shall include examination of applicable program requirements, operations, parts, devices, materials, software, and documentation to determine compliance with established requirements. The contractor shall document rationale for reductions in frequency or scope of evaluation. Results of evaluations, with recommendations for corrective action, shall be documented and stored in IDE (3.1.5). Follow-up shall be performed to verify effective corrective action has been taken. The contractor shall allow for the cognizant MDA Program Office and designated representative(s) access (3.1.14) and participation in supplier evaluations of hardware, processes, and software suppliers.

3.13.4 Supplier Program Requirements

The contractor shall establish and maintain a system specifying applicable program requirements and MAP requirements to suppliers. The system shall provide criteria for selection and flow down from contractor to supplier of MAP requirements imposed by prime contractor contract. These requirements shall reflect specific program phases based on considerations of item complexity and criticality. The contractor shall specify in the procurement document, applicable MAP requirements imposed on the supplier, using [Appendix A.2](#), Requirements Applicability Matrix (RAM). Suppliers shall then impose requirements on their procurement sources, also using [Appendix A.2](#). The RAM(s) flowed down to suppliers shall be stored in IDE (3.1.5).

3.13.4.1 Supplier Management System

The Government and prime contractor shall be responsible for documenting, tracking, monitoring, verifying, and auditing MAP and other technical requirements flowed down throughout the supply chain for all safety and mission critical hardware and software. Supplier's planning documentation shall be stored in prime contractor's IDE (3.1.5). Contractor's supplier management system shall contain provisions for the following requirements:

- a. Prime contractor shall establish and maintain a supply chain diagram based on bills of materials for all safety (3.14.1.2.2) and mission critical items (3.5.7), processes (3.12.2.2), and software (3.3.2.1).
- b. Prime contractor shall establish documented criteria for flow down of MAP and technical requirements. Tools used for requirements flow down and traceability shall ensure consistent application of criteria. Tools shall identify MAP and other technical requirements flow down for each supply chain tier.
- c. Suppliers shall identify and document critical processes and key characteristics. Suppliers shall provide a product critical processes and key characteristics document to the prime contractor containing the following information:
 - 1) Verification Matrix indicating how requirements are met for each critical process and key characteristic (e.g., dimensional and visual inspections or contractor approved acceptance test procedures). The Verification Matrix shall also specify the method (i.e., inspection, test, analysis, or demonstration) used to control each critical process and key characteristic.
 - 2) Standards (e.g., military standards, industry standards, contractor standards, and supplier standards) used for controlling safety and mission critical assemblies.
 - 3) All process controls and metrics used to monitor quality for each critical process and key characteristic.

- d. Prime contractor shall review and audit all supplier's critical processes and key characteristics and ensure process controls are in place. Additionally, prime contractor shall perform periodic audits of MAP and other technical requirements implementation. Audit results shall be documented and all problems or issues tracked to resolution. Critical or major problems or issues shall be elevated to top-level management, the cognizant MDA Program Office, and included for discussion at periodic program reviews. Review and audit results shall be an input to supplier chain metrics to monitor, control, and report supply chain health to the cognizant MDA Program Office.
- e. Supplier chain metrics shall provide continual health monitoring of supply chain implementation of MAP and technical requirements.
- f. Prime contractor shall store in IDE (3.1.5), a quarterly Supplier Management report based upon supplier inputs. The Supplier Management report shall include items a through e above and the following:
 - 1) Supplier identification and prime contractor assessment of supplier chain implementing documentation (e.g., process documentation, standards, command media, and procedures) for compliance to MAP requirements.
 - 2) Specific accountability and responsibility throughout the supply chain for implementation and verification of MAP and technical requirements.
 - 3) Documented validation process to ensure products meet requirements.
 - 4) Bi-directional requirements traceability for all safety and mission critical items throughout the supply chain.

3.13.5 Procurement Process

The contractor shall establish and maintain a process for generation, review, and release of procurement documents. This process shall be used to satisfy the contractor's responsibility for assuring supplier conformance to current configuration requirements. These controls shall be applied uniformly to all applicable suppliers and they shall include provisions for assurance of mutual notification of changes, verification of incorporation of changes, and identification of hardware, software, and services involved.

3.13.5.1 Technical Requirements

Procurement documents shall include SAE AS9100 requirements and these supplemental technical requirements:

- a. Interface, special tooling, and test and measuring equipment.
- b. Specifications for special preservation and packaging.
- c. Supplier notification to the contractor of any proposed changes to contractor approved design, parts, devices, materials, fabrication and test methods, or processes, and to obtain contractor approval before change incorporation.

3.13.5.2 Detailed Provisions

The contractor shall include these statements, or equivalent, in the procurement document:

- a. Government Source Inspection (GSI). The GSI is required before shipment. Upon receipt of this order, promptly notify the local Government representative so that appropriate planning for Government inspection can be accomplished.

- b. Procurements Not Requiring GSI. The Government has the right to inspect any or all of the work included in this order at the supplier's facility.
- c. Contractor Source Inspection. A contractor source inspection statement when source inspection is to be used.
- d. Raw Materials. Chemical and physical test results shall be submitted with a certificate of compliance. Purchased raw materials, which are required to satisfy documented specifications, shall be accompanied by a detailed analysis report.
- e. Raw Materials Used in Purchased Items. Records of detailed results of chemical and physical analyses of acceptance test results on raw materials required to satisfy specification requirements employed in the manufacture of articles purchased on this contract or purchase order shall be maintained by the supplier and made available upon request.
- f. Process Control and Inspection. Evidence of process controls and specific tests or inspections shall be provided to (contractor). Records shall be maintained by (supplier), adequate to ascertain the quality level of production processes.
- g. Limited Life Items. Items determined to have characteristics susceptible to quality degradation with age or storage environment shall be marked in a manner to indicate date of manufacture, date at which useful life was initiated and will expire, and specific storage environmental restrictions.
- h. Resubmission of Rejected Items. All items rejected by (contractor) and subsequently resubmitted by (name of supplier) shall bear an adequate indication of such resubmission on those items or on the shipping document. Reference shall be made to the (contractor) rejection document and evidence given that the causes for rejection have been corrected and actions taken to preclude recurrence.
- i. Certification of Manufacturer. All items to be submitted by (name of distributor) shall be accompanied by a certification of the name and location of the item manufacturer.
- j. Supplier Requirements and Review. The (supplier) shall, in the performance of the contract or purchase order, provide and maintain a program, which is in conformance with the following applicable program and QSMA requirements (attached). The (cognizant MDA Program Office), MDA/QS, and (contractor) may review (supplier) facilities to establish conformance to applicable program requirements.
- k. Product Changes. The supplier shall notify (contractor) of proposed changes to products including changes in design, fabrication and test methods or processes, materials, and changes, which may affect the quality or intended end use of the item. The supplier shall submit these changes to (contractor) for processing and approval.

3.13.5.3 Procurement Document Review

The contractor shall establish and maintain a process for independent (e.g., engineering and quality) technical review to ensure procurement documents are complete and correct. This review shall be accomplished before release of the purchase order and shall ensure:

- a. Appropriate program requirements are specified.
- b. Technical requirements are included.
- c. Applicable detailed provisions are specified.
- d. The supplier is an approved source or that provisions to perform necessary tests and inspections are planned.

- e. Applicable qualification requirements are satisfied.

Procurement documents and referenced data shall be available to the Government representative for review to determine compliance with contract requirements and need for Government inspection at supplier facilities. These documents shall be furnished IAW instructions from the Government representative.

3.13.5.4 Procurement Document Change Control

The Government and contractor shall provide for control and approval of changes to drawings, test procedures, specifications, and other procurement documents, and for incorporation of approved changes. For items procured to Government or contractor design, control shall include assurance of notification of change to the supplier, verification of incorporation, and appropriate identification of those items on which the change is incorporated. When a supplier proposes changes to design, fabrication methods, or processes the supplier shall submit these changes to the contractor for review and approval.

3.13.6 Control of Customer/Government Furnished Material

The contractor shall establish and maintain documented procedures to control receipt, verification, handling, preservation, storage, and maintenance of customer/Government supplied material provided for incorporation into end items, or for related activities. Any such material that is lost, damaged, or is otherwise unsuitable for use, shall be recorded and reported to the customer/Government. The contractor shall verify quality of supplied items and services by performing inspections and tests either upon receipt at the contractor's facility or at the supplier facility. Verification by the contractor does not relieve the customer/Government of the responsibility to provide acceptable material. When the overall system includes components or subsystems furnished by the Government, the contractor shall be responsible for obtaining from the Government adequate reliability data on the items. When the contractor's examination of data or testing indicates that Government Furnished Material reliability is inconsistent with overall system requirements, the cognizant MDA Program Office shall be formally and promptly notified.

3.13.7 Government Source Inspection

The Government reserves the right to inspect, at the source, items not manufactured or services not performed at contractor facilities. The GSI performed at supplier facilities on items or services, shall not ordinarily constitute acceptance, replace contractor inspection, nor in any way release the contractor from their responsibilities for assuring quality of these articles. However, when direct shipments from supplier facilities are specified, GSI and acceptance may be performed at supplier facilities. The GSI and acceptance can only be requested by or under authorization of the cognizant MDA Program Office or contract administration office.

3.13.8 Contractor Source Inspection

The contractor shall ensure suppliers comply with requirements of procurement documents by means of contractor source inspection at the supplier's facility, when appropriate. The system shall include requirements for documenting, collecting, and submitting source inspection and surveillance procedures and data. Additionally, records of inspections and tests witnessed by the source inspector, including quantities witnessed and nonconformance data, disposition made of nonconforming items, and corrective actions required of suppliers shall be maintained. Periodic reports from the source inspector shall be provided to the contractor concerning supplier operations monitored, including problems found and corrective actions taken.

Source inspection shall be performed when any of these conditions apply:

- a. Items are being procured at a level of assembly that prevents verification of quality at contractor facilities.

- b. Manufacturing processes have an effect on the item such that quality cannot be determined solely by examination or test of the completed item at contractor facilities.
- c. Destructive tests are necessary at supplier facilities.
- d. Special test and inspection equipment and environments required cannot feasibly and economically be reproduced or made available at contractor facilities.
- e. Shipments of completed items are made to destinations other than the contractor's facility.

3.13.9 Receiving Inspection and Test

The contractor shall establish and maintain a receiving inspection and test system in compliance with SAE AS9100 and supplemented by the following:

- a. Inspection and test of purchased items, including Commercial-Off-The-Shelf/Non-Developmental Items, to verify compliance with specification and drawing requirements. The degree of inspection and testing performed shall be governed by article complexity; results from supplier, source, and previous receiving inspections; and product quality history.
- b. Adequate equipment and instructions are available to perform tests and measurements.
- c. Items have passed qualification, requalification, or first article tests.
- d. Verification that required tests and inspections by the supplier have been performed, that processes are controlled, and that required data have been provided. The contractor shall periodically validate test reports.
- e. Procured articles subject to age deterioration are clearly marked and supported by information regarding life expiration date and need for any special environmental controls.
- f. Prompt inspection of Government Furnished Materials (GFM), including provisions for prompt feedback to the procuring contracting officer, when nonconforming GFM is found.
- g. Proper handling of purchased articles, including segregation and identification of those items awaiting inspection or test, those which have been accepted, those which have been rejected, and those awaiting material review action.
- h. Evidence that required source inspection has been performed and required data has been submitted.
- i. Use of appropriate sampling plans, if applicable, including provisions for reduced and tightened inspection.

When the contractor has a dock-to-stock program, Certificates of Compliance and associated data shall be maintained and the items shall be positively identified to permit recall in the event of nonconformity to specified requirements. Additionally, the contractor's dock-to-stock program shall have documented criteria for supplier certification and decertification. The criteria shall include ongoing analysis of supplier failure data, field problems and failures, process control data, periodic audit results ([3.13.3](#)), organizational stability, and other appropriate indicators of the contractor's ability to objectively assess conformance to contractual requirements.

3.13.10 Intra-Corporate Work Transfers

Contractor's intra-corporate work transfers shall reflect prime contract program requirements, or the assigned corporation element shall be treated as a supplier and the provisions of supplier management shall apply.

3.14 Safety

Government and contractors shall establish and maintain a system safety program, which ensures system safety throughout all phases of the system's life. The program shall apply engineering and management principles, criteria, and techniques to optimize all aspects of safety within constraints of performance, schedule, and cost. Government and contractors shall comply with this provision when assigned development, manufacturing, integration, or test responsibilities. The system safety program shall ensure:

- a. Safety, consistent with mission requirements, is designed into the system in a timely, cost effective manner, minimizing retrofit actions.
- b. Hazards are identified, evaluated, and eliminated using safety engineering principles. Any residual risk is reduced to a level acceptable to MDA Safety Risk Acceptance Authority throughout the entire life of a system. Actions taken to eliminate hazards or reduce risks are verified and documented.
- c. Historical safety data, including lessons learned from other systems, are considered and used.
- d. Safety risks are considered in accepting and using new designs, materials, and production and test techniques.
- e. Changes in design, configuration, or mission requirements are accomplished in a manner that improves or maintains an acceptable safety risk level.
- f. Effectiveness of mitigations are re-evaluated throughout the life cycle of the system, including tests and exercises, and corrected as new technology provides better mitigations or eliminates the hazard entirely.

The requirements of this document shall not exempt programs from meeting service specific safety requirements levied upon them, or any other safety requirements imposed by law.

3.14.1 Safety Program Requirements

The Government and contractor shall establish and maintain a system safety management and engineering program IAW MIL-STD-882. The program shall cover all phases of the system life cycle.

3.14.1.1 Safety Policies

Government and contractors shall comply with the following requirements which supplement other MDA safety policies and requirements:

- a. Ensure a systematic hazard analysis process is conducted and documented IAW MIL-STD-882. The safety hazard analysis process shall include system and subsystem hardware, software, the environment in which the system will exist, and the intended use or application over the product's life cycle. The safety hazard analysis shall document and disclose known safety defects and deficiencies associated with the element/program. Mitigations for identified hazards shall be documented and verified. Mitigations shall follow the design order of precedence IAW MIL-STD-882.
- b. Establish and maintain policies and procedures for formal review and approval of Government and contractor generated safety risk assessments.
- c. Designate a qualified safety representative with specific responsibility for coordinating and executing a safety program within the Government's and contractor's scope of responsibility. This representative shall have the requisite training and experience to assess and analyze safety issues. The qualified safety representative is the person who has supervisory responsibility/technical approval authority for the system safety work. This safety representative shall have, at a minimum, a

Bachelor of Science degree in engineering, physics, mathematics, or other scientific/technical disciplines and a minimum of four years of system safety or related experience.

- d. Ensure the prompt and accurate reporting, investigating, tracking, and closure of all safety related mishaps, near misses, problems, nonconformances, and anomalies, as defined in MDA Instruction 6055.02-INS, Accident and Mishap Safety Investigations and Reporting.
- e. Ensure all personnel understand anyone present is authorized to suspend any activity that presents an immediate and unacceptable danger to personnel, property, or operations, without retribution. All suspension of activities shall be reported to MDA/QS as soon as practical, but no later than 24 hours.
- f. Ensure appropriate corrective actions have been implemented before restarting any activity that has been suspended due to unacceptable danger to personnel, property, or operations.
- g. Ensure compliance with all applicable Range Safety and Service Safety requirements.
- h. Ensure a safety impact analysis is conducted on all requests for variances (waivers or deviations), Engineering Change Proposals (ECP), and software changes for engineering baselines under configuration management ([3.10](#)).
- i. Support System Safety Working Groups (SSWG), including Government and contractor chaired working groups.

3.14.1.2 Safety Task Documentation

Government and contractors shall develop and maintain necessary documentation and supporting evidence to show implementation of a systematic safety program including:

- a. Coordination of safety risk assessments with other internal engineering disciplines as well as the cognizant MDA Program Office and system level safety organizations to ensure safety risks are properly identified and documented.
- b. Development and maintenance of safety reports ([3.14.1.2.1](#)).
- c. Documentation, contribution, and use of safety related lessons learned to enhance safety throughout MDA.

3.14.1.2.1 System Safety Program Plan

The Government and contractor shall establish and maintain a System Safety Program Plan (SSPP). The Government and contractor shall perform this effort IAW MIL-STD-882E, Task 102. The contractor's SSPP shall be prepared early in the program life cycle and submitted into IDE ([3.1.5](#)) and marked for approval by the cognizant MDA Program Office. Notification that the SSPP is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item. The SSPP shall be updated as required to maintain currency with program evolution. The SSPP shall:

- a. Describe the Government's and contractor's implementation of System Safety requirements defined herein. Describe tasks and activities of system safety management and engineering and the interrelationship between system safety and other functional elements of the program. Identify each hazard analysis and mishap risk assessment process that will be used.
- b. Describe methods used to identify and apply hazard control requirements and criteria for design of equipment, software, facilities, and procedures during the product's life.
- c. Specify analysis technique(s) and format used in qualitative and quantitative analysis to identify hazards, their causes and effects, and recommended corrective action.

- d. Specify depth within the system to which each analysis technique will be used, including hazard identification associated with system, subsystem, components, software, personnel, Ground Support Equipment (GSE), Government Furnished Equipment, facilities, and their interrelationship in logistic support, training, maintenance, transportability, security, and operational environments.
- e. Specify integration of supplier hazard analyses and techniques with overall system hazard analyses.
- f. Specify the technique for tracking hazards in a single closed loop system.
- g. Define how hazards and residual mishap risk are communicated to and accepted by the appropriate risk acceptance authority and how hazards and residual mishap risk will be tracked.
- h. Specify techniques and procedures used to ensure objectives and requirements of the system safety program are included in safety training for engineers, technicians, programmers, testers, operators, and maintainers.
- i. Specify safety techniques and procedures employed to ensure objectives and requirements of the system safety program are accomplished.
- j. Define the mishap analysis process, IAW MDA Instruction 6055.02-INS.
- k. Include an item-by-item accounting of all contractually required system safety requirements, tasks, and responsibilities.
- l. Include information on system safety integration into the overall program structure.
- m. Include the system safety organization or function within the organization responsible for System Safety, its functional relationships, and lines of communication.
- n. Include responsibility, authority, and accountability of system safety personnel, other Government and contractor organizational elements involved in the system safety effort, suppliers, and system safety groups.
- o. Include the organizational unit responsible for executing each system safety task, and the position with authority to resolve all identified hazards.
- p. Include staffing of the system safety organization for the duration of the contract/development agreement to include manpower loading and qualifications of assigned personnel.
- q. Include the process through which management decisions will be made to include notification of critical and catastrophic hazards, corrective action taken, mishaps or malfunctions, waivers to safety requirements, and program deviations.
- r. Include verification requirements for ensuring safety.
- s. Include procedures for ensuring:
 - 1) Feedback of test information for review and analysis on impact to safety.
 - 2) Safe conduct of all tests.
 - 3) Hazards identified have been eliminated or controlled to an acceptable level of risk.
 - 4) Controlled hazards are reviewed and re-evaluated for effectiveness of current mitigations.

- t. Include an integrated system safety schedule that supports the program's engineering and programmatic milestones.
- u. Include description of:
 - 1) Approach for identifying, obtaining, researching, disseminating, and analyzing pertinent historical hazard or mishap data.
 - 2) Interfaces between system safety and all other applicable safety disciplines, such as Nuclear Safety, Range Safety, Explosive and Ordnance Safety, Chemical and Biological Safety, Occupational Safety and Health, Laser Safety, Radio Frequency (RF) Safety, and Software Safety.
 - 3) Interfaces between system safety and all other support disciplines, such as Maintainability, Quality Assurance, Security, Reliability, Human Factors Engineering, Transportability Engineering, and Medical Support (Health Hazard Assessments).
 - 4) Procedures used to integrate and coordinate system safety efforts, including dissemination of system safety requirements to action organizations and suppliers, coordination of supplier's system safety programs, integration of hazard analyses, program and design reviews, program status reporting, and system safety groups.

3.14.1.2.2 System Safety Hazard Analysis and Report

The Government and contractor shall perform a system safety hazard analysis. The analysis shall:

- a. Identify safety critical functions. For each safety critical function, the Government and contractor shall establish a process for analysis, design, test, and verification and validation of those functions.
- b. Include tailoring and communication of safety requirements and constraints to system and software designers early in the acquisition process.
- c. Identify, document, and track system and subsystem level hazards and their effects, including the human as an element of the total system.
- d. Categorize each and every identified hazard in terms of severity and probability of occurrence per MIL-STD-882 criteria (specify qualification or quantification of likelihood).
- e. Identify each failure path and associated causal factors. This analysis shall be to the functional depth necessary to identify logical, practical, and cost effective mitigation techniques for each failure path initiator (causal factor). This analysis shall consider as potential contributors all hardware, software, and human factor interfaces. Based on causal factors on the failure path for catastrophic or critical safety hazards, develop a list of safety critical items ([3.13.1.1](#)).
- f. Derive safety specific hazard mitigation requirements to eliminate or reduce the likelihood of each causal factor.
- g. Provide engineering evidence (through appropriate inspection, analysis, demonstration, or test) that each mitigation safety requirement is implemented within design and system functions to meet safety goals and objectives. Any residual mishap risk shall be documented. All new hazards identified during testing shall be reported to MDA/QS and other cognizant MDA Program Offices.
- h. Evaluate all hardware, software, and firmware changes and defects for their potential safety impact.
- i. Communicate a safety assessment of all residual safety risk after all design, implementation, and test activities are complete.

The Government and contractor shall use the system safety hazard analysis report results to develop the safety assessment report (3.14.1.2.3). The contractor's safety assessment report shall be stored in IDE (3.1.5).

3.14.1.2.3 Safety Assessment Report

The Government and contractor shall perform and document a safety assessment to give a comprehensive evaluation of the residual mishap risk before any test event or initial operation of a system. Safety assessment shall also be performed and documented to identify all safety features of hardware, software, and system design and to identify procedural, hardware, and software related hazards that may be present in the system being acquired, including specific procedural controls and precautions that should be followed. The Safety Assessment Report (SAR) shall summarize:

- a. Safety criteria and methodology used to classify and rank hazards, including any tailoring of criteria or methodologies. Classification shall be accomplished IAW 3.14.3.3, Risk Acceptance Authority.
- b. Results of analyses and tests performed to identify hazards inherent in the system, including:
 - 1) Hazards having residual safety risk.
 - 2) Actions that have been taken to mitigate or eliminate hazards.
 - 3) Validation of safety criteria, requirements, and analyses.
- c. Results of safety program efforts. Include a list of all hazards along with specific safety recommendations or precautions required to ensure safety of personnel, property, or environment. Categorize the list of hazards as to whether or not they may be expected under normal or abnormal operating conditions.
- d. Any hazardous materials generated by or used in the system, including:
 - 1) Identification of material type, quantity, and potential hazards.
 - 2) Safety precautions and procedures necessary during use, packaging, handling, storage, transportation, and disposal. Include all explosive hazard classifications.
 - 3) Post launch safety related activity of expendable launch vehicles and their payloads including deployment, operation, re-entry, and recovery (if required) of launch vehicles/payloads, which do not attain orbit (either planned or unplanned).
 - 4) Orbital safety hazard awareness associated with space systems such as explosions, electromagnetic interference, radioactive sources, ionizing radiation, chemicals, space debris, safe separation distances between space vehicles, and natural phenomena.
 - 5) A copy of the Material Safety Data Sheet (OSHA Form 174, or equivalent manufacturer's format).
 - 6) Hazardous spill/release response plan.

The Government and contractor shall conclude the safety assessment report with a signed statement confirming all identified hazards were eliminated or their residual risks controlled to levels acceptable to the cognizant MDA Program Offices and the system is ready to test, operate, or proceed to the next acquisition phase. Additionally, the Government and contractor shall make recommendations applicable to potential hazards at interfaces with other BMDS programs. The contractor shall ensure results of safety assessments and supporting data are stored in IDE (3.1.5) for review and information for the cognizant MDA Program Office, MDA/QS, and appropriate safety review boards. Engineering support

shall, as requested, be provided to MDA/QS to facilitate assessment and acceptance of identified residual risks at the appropriate level.

3.14.1.2.4 Safety Variance (Waiver/Deviation) Reporting

The contractor shall submit proposed variances (waivers or deviations) affecting safety requirements to the cognizant MDA Program Office, MDA/QS, and appropriate safety review boards for review and comment before submittal to the variance approval authority. Variances affecting safety requirements shall be dispositioned IAW [3.10.4.6.3](#). The risk associated with variances shall be accepted IAW [\(3.14.3.3\)](#). Approval or disapproval of variances affecting safety requirements shall be reported to the cognizant MDA Program Office, MDA/QS, and appropriate safety review boards following their disposition by the approval authority. The Government and contractor shall provide requested information to facilitate acceptance of variances requiring MDA approval/acceptance in time to meet mission schedules. The contractor's safety variances shall be stored in IDE [\(3.1.5\)](#).

3.14.1.2.5 Engineering Change Proposal System Safety Reports

Government and contractor shall conduct a safety impact assessment on all hardware, software, and firmware change requests, variances (waivers or deviations), and ECPs for products under configuration control. The contractor shall prepare and submit Hazard Analysis Reports and/or SARs associated with ECPs and variances into IDE [\(3.1.5\)](#) and marked for approval by the cognizant MDA Program Office. Notification that Hazard Analysis Reports and/or SARs associated with ECPs and variances are submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

3.14.1.2.6 Integrated System Safety Program Plan

Government or contractor designated as integrator for the safety functions shall establish and maintain an Integrated System Safety Program Plan (ISSPP) defining the role of the integrator and effort required from each supplier to help integrate system safety requirements for the total system. The contractor's ISSPP shall be submitted into IDE [\(3.1.5\)](#) and marked for approval by the cognizant MDA Program Office. Notification that the ISSPP is submitted for review and approval shall be issued to organizations listed on the Contract Data Requirements List item.

The ISSPP shall address and identify:

- a. Control, authority, and responsibility transitions from contractor to suppliers.
- b. Analyses, risk assessment, and verification data to be developed by each supplier, and format and method to be used.
- c. Data each supplier is required to submit to the integrator and its scheduled delivery keyed to program milestones.
- d. Schedule and acquisition planning pertinent to the integrator.
- e. The development method of system and software level requirements allocated to each supplier as part of the system specification, end item specifications, and other interface requirement documentation.
- f. Safety related data pertaining to Legacy Designs, Non-Developmental Items and Commercial-Off-The-Shelf hardware and software.
- g. Integrated safety analyses to be conducted and support required from suppliers.
- h. Government's and contractor's roles in test range, nuclear safety, explosive, or other certification processes.

3.14.1.2.7 Health Hazard Assessment Report

The contractor shall identify, evaluate, and document safety and health hazards, define risk levels, and establish a program that manages probability and severity of all hazards associated with development, use, and disposal of the system (3.14.4). The contractor shall perform this effort IAW MIL-STD-882E, Task 207. The Health Hazard Assessment Report shall be documented and available via IDE (3.1.5).

3.14.1.2.8 Safety Incident/Near Miss Report

The Government and contractor shall create a Safety Incident/Near Miss Report for MDA/QS. The contractor's Safety Incident/Near Miss Report shall be stored in IDE (3.1.5). Government shall investigate and report mishaps involving MDA programs or program assets IAW MDA Instruction 6055.02-INS, Accident and Mishap Safety Investigations and Reporting. Contractors shall support mishap investigations, as required. Safety Incident/Near Miss Reports shall include:

- a. Test, Training, and Exercise (TT&E) data introduced into safety critical environments.
- b. TT&E data mislabeled as real.
- c. Failures of safety inhibits.
- d. On-the-job injuries.
- e. Inadvertent arming.
- f. Inadvertent radiation.
- g. Equipment damages over \$200K.
- h. Fires.
- i. Flooding of facilities.
- j. Violations of safety procedures.
- k. Natural incidents (e.g., earthquakes, tsunamis, mud slides, hurricanes, and tornados). Prior to resuming operations, ensure facilities related to MDA production and operations are capable of safely resuming activities following the incident.

3.14.1.2.9 Management Trends Reports

The contractor shall alert the cognizant MDA Program Office via monthly Management Trends Reports when any of the following occur:

- a. Turnover of safety personnel.
- b. Reductions in safety workforce.
- c. Modifications to safety processes.
- d. Summary of new hazards and mitigations.

The contractor's monthly Management Trends Reports shall be stored in IDE (3.1.5).

3.14.1.2.10 Message Modification Technologies Reporting and Approval

The Government and contractor shall identify any use of message modification technologies IAW MDA Policy Memorandum 72.

3.14.1.3 System Safety Working Groups

The Government and contractor shall form and support SSWGs with input from the subcontractors to address all aspects of safety including, but not limited to:

- a. System safety.
- b. Test and evaluation safety.
- c. Software safety.
- d. Range safety.
- e. Occupational safety and health.

The contractor may form and lead working groups with their subcontractors and suppliers, as needed ([3.14.1.2.6](#) and [3.14.12.2](#)).

3.14.1.4 Hazard Tracking

The contractor shall establish and maintain a hazard tracking system with current safety data including hazards, their closures, and residual mishap risk throughout the system life cycle. The contractor shall provide the cognizant MDA Program Office and MDA/QS access to the hazard tracking system. The hazard reporting topics shall include:

- a. Conditions related to the hazard (e.g., mode of operation, operational environment, and configuration).
- b. Consequences - description of damage or loss and its severity.
- c. Likelihood of hazard mishap occurring.
- d. Milestone when the hazard becomes relevant or is no longer relevant.
- e. Proposed mitigations - implementations that lower likelihood or severity of the mishap.
- f. Updates as mitigations are implemented.
- g. Updates as the mitigations are verified and validated.

3.14.1.5 Safety Verification

The Government and contractor shall verify mishap risk mitigation through appropriate analysis, testing, or inspection. The Government and contractor shall document residual mishap risk and shall report all new hazards identified during testing to the cognizant MDA Program Director or Program Manager and MDA/QS via a system safety hazard analysis report. The contractor's report shall be stored in IDE ([3.1.5](#)). The Government and contractor shall review mitigations at least annually to ensure effectiveness.

3.14.1.6 Safety Defect/Deficiency Assessment

The Government and contractor shall review all known hardware, software, and firmware defects and deficiencies for potential safety implications. If safety impacts are identified, the Government and contractor shall immediately notify MDA/QS and the cognizant MDA Program Office of a decrease in the level of system safety. The contractor's defects and deficiencies impacting safety shall be included in the Hazard Analyses and SARs and stored in IDE ([3.1.5](#)).

3.14.1.7 System Safety Program Reviews/Audits

Government and contractors shall perform and document system safety program reviews and audits. These requirements supplement requirements in [3.1.8](#), Internal Evaluation Program. These reviews and audits shall be performed on Government's and contractor's system safety programs. The contractor's review and audit results shall be stored in IDE ([3.1.5](#)).

The Government and contractor shall support presentations to Government assessment activities such as safety reviews, munitions safety boards, or flight safety review boards, and may also include special reviews such as flight or test readiness reviews.

The Government and contractor shall use desk audits, peer reviews, static and dynamic analysis tools and techniques, and debugging tools to verify implementation of design requirements in the source code with particular attention on implementation of identified safety critical computing system functions. Reviews of software source code shall ensure agreement between code and comments within code.

3.14.2 System Safety Requirements

The contractor shall identify and understand known hazards and their associated risks. Hazard analysis and safety risk management IAW MIL-STD-882 shall be performed by the contractor to achieve acceptable safety risk. The contractor shall identify and establish potential mishap risk mitigation alternatives and expected effectiveness of each alternative or method for each risk.

The order of precedence for system safety hazard control shall be IAW MIL-STD-882.

3.14.3 System Safety Engineering Approach

The contractor's system safety program shall support the general process outlined in Figure 3.14.3-1.

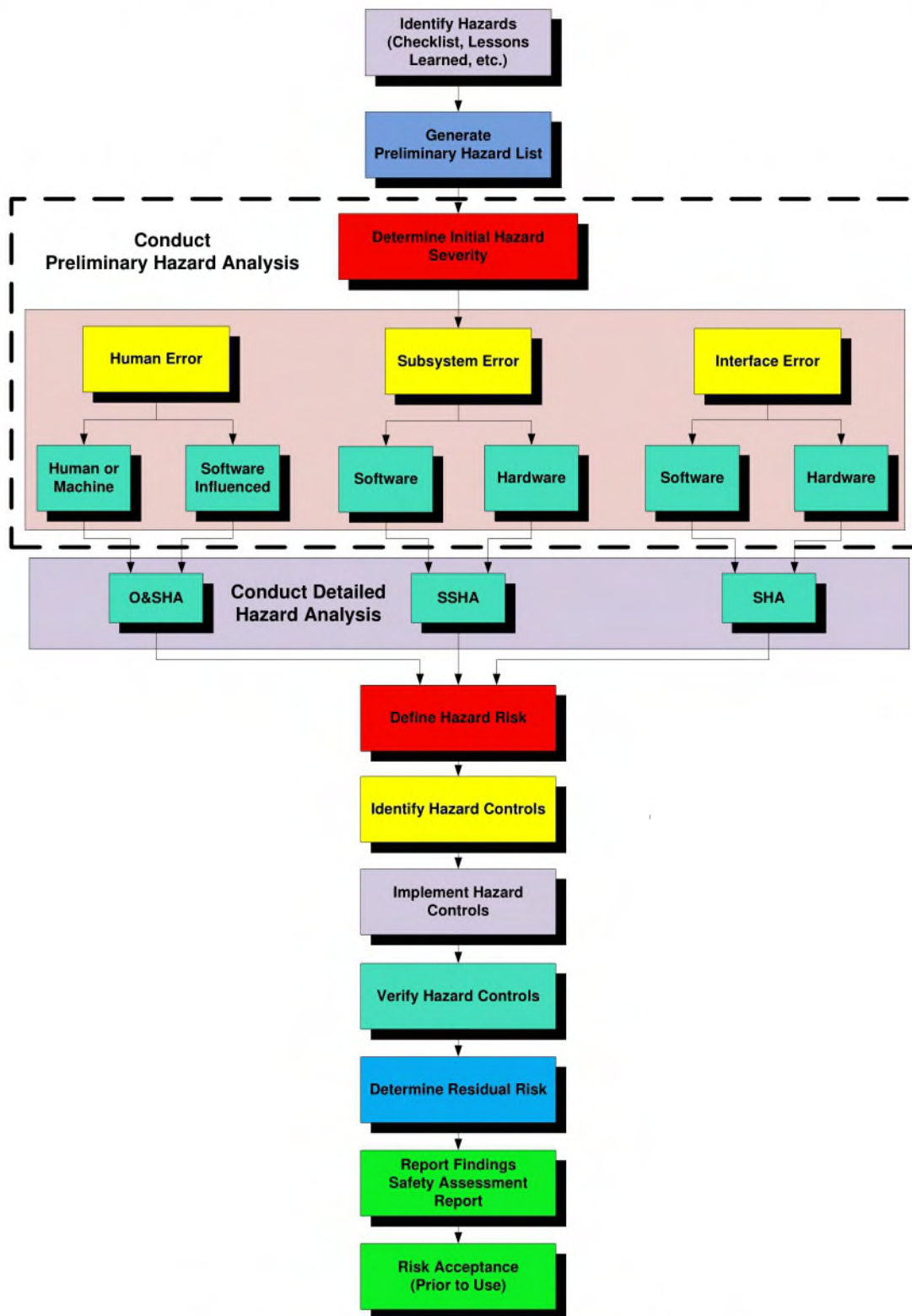


Figure 3.14.3-1 System Safety Engineering Approach

3.14.3.1 System Safety Hazard Identification and Analysis Methodology

The contractor shall perform safety analyses to identify hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware, software, and firmware, the environment in which the system will exist, and intended use or application. The contractor shall use historical hazard and mishap data, including lessons learned from other systems, and during hazard identification, consider hazards that could occur over the system life cycle.

The contractor shall establish a hazard analysis methodology to identify and document specific elimination, mitigation, or control requirements to ensure residual safety risk is acceptable to MDA and the cognizant MDA Program Office. For every hazard causal factor identified that increases potential for mishap, there shall be specific mitigation planning identified to successfully control the mishap or hazard to acceptable levels. When multiple hazard control requirements are identified, they shall be prioritized IAW the hazard control order of precedence defined in [3.14.2](#).

3.14.3.2 Assessment of Mishap Risk

The Government and contractor shall assess and document risks IAW MIL-STD-882E Section 4, General Requirements.

3.14.3.3 Risk Acceptance Authority

The Government shall submit to the proper authority for acceptance, all safety risks which are not eliminated through design or documented user accepted procedures. Table 3.14.3.3-1 shows the acceptance authority for all safety risks during development, operation, and maintenance of the BMDS and BMD elements.

Note: MDA acceptance of safety risks does not imply that Test Range(s) will accept these risks for tests.

Risk Level Per MIL-STD-882E Tables III and VI	Safety Risk Acceptance Authority
High	MDA Director
Serious	MDA Executive Director
Medium	Program Director or Director for Test (MDA/DT)
Low	Program Director or Director for Test (MDA/DT)

Table 3.14.3.3-1 Safety Risk Acceptance Authority

Residual safety risks can be accepted only by the proper level of management within MDA. Safety risk acceptance authority cannot be delegated to any subordinate level of management. Residual safety risk acceptance should occur at least 30 days before major milestone decisions and, in all cases, residual risk shall be accepted before it is actually experienced. Program Directors or MDA/DT shall formally brief the High and Serious element residual risks to appropriate risk acceptance authority, as defined in the MDA Safety Risk Acceptance Authority Memo, and prepare an acceptance letter for signature. Formal user representative coordination shall be provided. Briefings and residual risk acceptance letters shall be pre-coordinated with MDA/QS, who developed standard formats for such, and will also attend the briefing and provide recommendations.

3.14.3.4 Mishap Investigations

The Government shall investigate and report mishaps involving MDA programs, IAW MDA Instruction 6055.02-INS. The contractor shall support mishap investigations. The contractor's investigation results shall be stored in IDE ([3.1.5](#)).

3.14.4 Safety Design Criteria

The contractor shall comply with the following design requirements which supplement provisions [3.2](#), Design and Development, and [3.3](#), Software and Firmware. Compliance with requirements in this section shall be reflected in the SSPP and the contractor's Software Coding Standard. The contractor shall identify and rank hazards inherent in the system. Once the hazards have been identified, mitigations shall be proposed for each hazard to reduce the overall risk level to one that is acceptable to the cognizant MDA Program Office and MDA/QS.

3.14.4.1 Unacceptable Conditions

The contractor's design shall eliminate the following unacceptable conditions:

- a. Single component failure, common mode failure, human error, or a design feature that could cause a mishap of Catastrophic or Critical mishap severity.
- b. Dual independent component failures, dual independent human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of Catastrophic or Critical mishap severity.
- c. Generation of hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.
- d. Packaging or handling procedures and characteristics that could cause a mishap of severity category 1, 2, or 3 for which no controls have been provided to protect personnel or sensitive equipment.

3.14.4.2 Design Constraints

The contractor's design shall comply with the following constraints:

- a. For non-safety critical command and control functions: a system design that requires two or more independent human errors, each resulting from independent sources of information, or that requires two or more independent failures, or a combination of independent failure and human error to lead to a mishap.
- b. For safety critical command and control functions: a system design that requires at least three independent failures, or at least three independent human errors, or a combination of at least three independent failures and human errors to lead to a mishap.
- c. System designs that positively prevent errors in assembly, installation, or connections that could result in a mishap.
- d. System designs that positively prevent damage propagation from one component to another, or prevent sufficient energy propagation to cause a mishap.
- e. System design limitations on operation, interaction, or sequencing that preclude occurrence of a mishap.
- f. System designs that provide an approved safety factor that limits possibilities of structural failure or release of energy sufficient to cause a mishap ([3.14.3.2](#)).
- g. System designs that control energy build-up that could potentially cause a mishap (e.g., fuses, relief valves, or electrical explosion proofing).
- h. System designs where component failure can be temporarily tolerated because of residual strength or alternate operating paths, so that operations can continue with a reduced but acceptable safety margin.

- i. System designs that positively alert controlling personnel to a hazardous situation where capability for operator reaction has been provided.
- j. System designs that limit or control use of hazardous materials.
- k. System designs that revert to a safe state in the event of an interruption or loss of power or the loss of the computing system.

3.14.4.3 Interlock Status and Restoration

The contractor shall design interlocks to preclude hazards to personnel maintaining potentially hazardous systems. Where interlocks must be overridden to perform tests or maintenance, they shall be designed so they cannot be inadvertently overridden or left in the overridden state once the system is restored to operational use. The override of the interlocks shall not be controlled by a computing system. The status of safety interlocks shall be prominently displayed to the operator at all times.

3.14.4.4 Ignition System Safety Requirements

The contractor shall design rocket motor ignition systems IAW MIL-STD-1901. Contractors shall store compliance verification documentation in IDE [\(3.1.5\)](#).

3.14.4.5 Fuze System Safety Requirements

The contractor shall design and test fuze systems IAW MIL-STD-1316. Contractors shall store compliance verification documentation in IDE [\(3.1.5\)](#).

3.14.4.6 Hazardous Materials Transportation

The contractor shall design, test, classify, and transport hazardous materials systems IAW 49 CFR Parts 100-185, Technical Bulletin (TB) 700-2/ NAVSEA INST 8020.8/TO11A-1-47/DLAR 8220.1, and, as applicable, NAVSEAINST 9310.1B. The contractor is responsible for obtaining required documentation to ship hazardous material.

3.14.4.6.1 Lithium Batteries

The contractor shall:

- a. Perform a Safety Transportation analysis and obtain a Certificate of Equivalency (COE) certification per Defense Transportation Regulation, DTR 4500.9-R, for all Lithium batteries prior to Program Critical Design Review. A COE is an approval issued by the DOD for instances where a packaging design differs from the prescribed regulations in 49 CFR. A COE certifies that the proposed packaging design equals or exceeds the comparable requirements of 49 CFR for the commodity being shipped.
- b. Comply with S9310-AQ-SAF-010, Technical Manual for Batteries, Navy Lithium Safety Program Responsibilities and Procedures, Rev 2 Dated 15 July 2010. Although this document is specific to Navy systems, it shall be applied to all MDA systems using Lithium cells/batteries.

3.14.4.7 Insensitive Munitions Design and Safety Tests

The contractor shall design and test munitions systems IAW:

- a. Public Law (United States Code), Title 10, Chapter 141, Section 2389, Armed Forces Miscellaneous Procurement Provisions: Ensuring Safety Regarding Insensitive Munitions.
- b. MIL-STD-2105, Section 5.2, Hazard Assessment Tests for Non-Nuclear Munitions.

- c. TB 700-2/NAVSEAINST 8020.8B/TO 11A-1-47/DLAR 8220.1, DOD Ammunition and Explosives Hazard Classification Procedure.

3.14.4.8 Ordnance Systems

The contractor shall develop and handle ordnance IAW DOD 4145.26-M. All electroexplosive devices shall be developed and handled IAW MIL-STD-1576.

3.14.4.9 Missile and Space Vehicle Pressure Systems

The contractor shall develop missile and space vehicle pressure systems and their associated GSE IAW MIL-STD-1522 and AIAA S-080. For metal-lined composite pressure vessels, the contractor shall also comply with AIAA S-081.

3.14.4.10 Orbital Debris

The Government and contractor shall minimize orbital debris, per US Government Orbital Debris Mitigation Standard Practices, and shall give consideration to NASA Safety Standard 1740.14, Guidelines and Assessment Procedures for Limiting Orbital Debris.

3.14.5 Safety and Health

The Government and contractor shall identify and evaluate safety and health hazards, define risk levels, and establish a program that mitigates probability and severity of all hazards associated with development, use, and disposal of MDA systems. The Government and contractor shall use the system safety program to manage safety and health risks encountered in the acquisition process of systems, subsystems, equipment, and facilities. These risks include conditions that create risks of death, injury, acute/chronic illness, disability, or reduced job performance of personnel who produce, test, operate, maintain, support, or dispose of the system.

3.14.5.1 Occupational Safety and Health

The Government and contractor shall manage Occupational Safety and Health (OSH) and ensure compliance with applicable federal, state, and local laws and regulations, to mitigate OSH risks, as required by industry and DOD standards. The Government and contractor shall address OSH regulations in each phase of a system's life cycle. The OSH applicable requirements shall be integrated into the systems engineering process (3.2.4) and risk management program (3.1.6). The Government and contractor shall conduct OSH risk assessments associated with:

- a. Hazardous Materials Management.
- b. Human Engineering.
- c. Lasers.
- d. Human Exposure to RF.

The risk assessment criteria shall be consistent with Risk Acceptance Authority 3.14.3.3. The Government and contractor shall support Programmatic Environmental, Safety & Health Evaluations (PESHE).

3.14.5.1.1 Hazardous Materials Management

The contractor shall establish and maintain a Hazardous Material Management Program (HMMP) to eliminate or reduce use of hazardous materials in processes and products and tracking, storing, handling, packaging, transporting, and disposing of such material IAW MIL-STD-882E, Task 108. The contractor's

Health Hazard Analysis IAW MIL-STD-882E, Task 207 shall be prepared and stored in IDE (3.1.5). A copy of the Material Safety Data Sheet (OSHA Form 174) for each material shall be accessible to personnel involved in handling, shipping, or storage of hazardous materials.

3.14.5.1.2 Human Engineering

The contractor shall use MIL-STD-1472 to establish effective procedures, work patterns, and personnel safety and health, and to minimize factors, which degrade human performance or increase error. The contractor shall ensure design induced requirements for operator workload, accuracy, time constraint, mental processing, and communication do not exceed operator capabilities.

3.14.5.1.3 Lasers

The contractor shall design and operate lasers IAW ANSI Z136.1 and ANSI Z136.6.

3.14.5.1.4 Human Exposure to Radio Frequency

The contractor shall design and operate systems to limit personnel exposure to RF energy IAW IEEE C95.1. The contractor shall evaluate and document hazards to aircraft and satellite electronics and mitigate hazards to an acceptable level (3.14.3.3).

3.14.6 Test and Range Safety

The Government and contractor shall incorporate test safety considerations into their design and test planning efforts as described in 3.14.6.1 and 3.14.6.2. In the event of conflict between MAP requirements and Range Safety requirements, the Government and contractor shall comply with the more stringent requirements.

3.14.6.1 Test Safety

The Government and contractor shall ensure test and evaluation safety activities reduce, correct, or control hazards in the test and evaluation environment. Acceptance of residual safety risk for MDA tests shall be accomplished IAW 3.14.3.3. These testing requirements supplement those contained in provisions 3.3.2.5 and 3.7. Specific test and evaluation safety activity tasks shall include:

a. Test and Evaluation Planning. Planning for test and evaluation safety shall include:

- 1) Test program milestones requiring completion of hazard analyses, risk assessments, or other safety studies.
- 2) Schedule for analysis, evaluation, and approval of test plans, procedures, and other documents to ensure safety is covered during all testing.
- 3) Preparation of, or input to, safety, operating, and test procedures.
- 4) Coverage of test equipment, installation of test equipment, and instrumentation in hazard analyses before test commencement.
- 5) Specialized requirements designated by the cognizant MDA Program Office and MDA/DT.
- 6) Informing the cognizant MDA Program Office, MDA/DT, and MDA/QS of any identified hazards that are unique to the test environment.
- 7) Coordination and status reviews with the cognizant test site safety representative(s) to ensure test safety requirements are identified, monitored, and completed, as scheduled.

- b. Safety Assessments. The Government and contractor shall conduct safety assessments and hazard analyses IAW MIL-STD-882 to address test and evaluation specific safety concerns.
- c. Safety Reviews. The Government and contractor shall provide assistance to safety review teams to support an independent safety review that will, from a safety perspective, validate the system is ready to test.
- d. Follow-up Actions. The Government and contractor shall:
 - 1) Analyze and document safety related test results.
 - 2) Initiate follow-up action to ensure completion of corrective efforts taken to reduce, correct, or control test and evaluation hazards.
- e. Reports. The Government and contractor shall maintain a repository of test and evaluation hazard/action status reports. Contractor reports shall be stored in IDE [\(3.1.5\)](#).

3.14.6.2 Range Safety

The Government and contractor shall comply with applicable Range Safety requirements to assure the general public, launch area personnel, foreign land masses, and launch area resources are provided a level of safety acceptable to Range Safety, and that all aspects of pre-launch, launch, and post-launch operations adhere to public laws and national needs.

The Government and contractor shall meet Range Safety requirements for each and every range where they intend to test. The Government and contractor shall support tailoring of Range Safety requirements. The AFSPC Manual 91-710 will be used as a baseline for this tailoring effort. Any variance to tailored Range Safety requirements shall require written approval from every affected party, including Range Safety.

For MDA test operations that occur at a non-National range, a National Range and its associated range safety requirements shall be selected by the cognizant MDA Program Office and MDA/QS, and used to supplement requirements of the non-National range.

A lead range shall be identified by MDA/DT for MDA test operations involving multiple ranges. That lead range will be responsible for assuring overall range safety for the mission. Special attention shall be given to operational hand-offs between ranges for specific flight tests. Critical considerations include command codes and handover points and interchange of real-time tracking and telemetry data. Command handovers shall be automated to minimize latency. These hand-off processes and procedures shall be positively verified before launch of each test vehicle.

In addition to previous requirements, the following apply to multiple ranges and multiple vehicle operations:

- a. Each launch vehicle requiring flight termination capability shall have flight termination design and procedures, which preclude the possibility of destroying the wrong vehicle during simultaneous flight, or while a vehicle or vehicles are flying and another, or others, are on the ground. Command and channel check tones shall be coordinated between ranges to prevent inadvertent commands.
- b. The Government and contractor shall meet requirements of RCC-324-01.
- c. MDA test operations shall require two independent, non-common and adequate range tracking sources.

The Government and contractor shall comply with Lightning Launch Commit Criteria, documented in Aerospace Report No. TR-99 (1413)-1.

3.14.6.2.1 Flight Termination System and Range Safety Tracking System Standards

The contractor shall design, test, and deliver flight termination systems (FTS), global positioning and inertial measurement range safety tracking systems, transponder tracking systems, and telemetry systems that comply with these standards, as jointly required and tailored by all affected ranges:

- a. RCC-319, Flight Termination Systems Commonality Standard.
- b. AFSPC Manual 91-710, Range Safety User Requirements Manual (Vol. 1-7).
- c. RCC-106-01, Telemetry Standards.

3.14.6.2.2 Three-Tone Receivers

The Government or contractor shall not use three-tone FTS receivers for new designs on MDA test flight hardware unless approved by the MDA/QS Director. If three-tone FTS receivers are approved, then operational implementation of command transmissions used by the range in lieu of the check channel tone, or for any other in-flight actuated commands, shall be documented, presented, and approved by the MDA/QS Director or designated representative(s). The contractor shall implement a plan to eliminate legacy test flight hardware currently utilizing three-tone FTS receivers and employ four-tone, or more advanced technologies, at the earliest practical time.

3.14.6.2.3 FTS Receiver Implementation Exclusivity

The Government's or contractor's use of FTS receivers on new flight test vehicles shall be solely to execute Range required flight termination command and monitor functions. Additional flight commanded operational functions may be implemented with range concurrence and coordination, but shall use separate Range Commanders Council (RCC) Inter-Range Instrumentation Group (IRIG) tone decoding receivers. Such additional receivers shall be electrically and operationally isolated from command destruct functional receivers and will not use any RCC (IRIG) tones for RF uplinked functions that are in common with those used for range FTS command or monitor functions.

3.14.6.2.4 Flight Safety Analysis

The Government or contractor shall perform flight safety analysis IAW requirements of affected Ranges or tailored RCC-321-10. These analyses shall be stored in IDE [\(3.1.5\)](#).

3.14.7 Safety Critical Computing System Functions

The contractor shall designate the required safety functions of the computing system as Safety Critical Computing System Functions (SCCSF). The SCCSFs are defined as those computer functions in which an error can result in a mishap or accident. Safety critical functions of computing systems include not only control functions where the computer exercises direct control over a system, but those where the output information is used to make safety critical decisions, manually or automatically, locally or remotely, by another system and its operator.

The SCCSFs include any function that:

- a. Controls or directly influences pre-arming, arming, enabling, release, launch, firing, initiation of munitions or directed energy system.
- b. Determines, controls, or directly influences flight path of a munitions system or beam path of a directed energy system.
- c. Controls or directly influences movement of gun mounts, launchers, and other equipment.
- d. Controls or directly influences movement of munitions and hazardous materials.

- e. Monitors state of the system for purposes of ensuring its safety.
- f. Senses hazards and displays information concerning protection of the system.
- g. Controls or regulates energy sources in the system.
- h. Generates, controls, routes, or modifies data that are used by operators or another system to perform a safety critical task.

Additional functions may be considered to be SCCSF, depending on the software implementation in system context. The contractor shall perform a hazard analysis of risks associated with specified functions of the computing system IAW MIL-STD-882. Contractor's results of this analysis shall be stored in IDE [\(3.1.5\)](#).

All implementations of safety critical computing functions, mitigations, and requirements shall be evaluated for robustness and be verified and validated for intended use and environment [\(3.3.3.5\)](#). These activities shall be performed by an organization which is managerially, financially, and technically independent of the developer. Contractor's evaluation results shall be stored in IDE [\(3.1.5\)](#).

3.14.8 Safety Critical Variables and Information Exchange Requirements

The contractor shall identify and track all safety critical variables and Information Exchange Requirements (IER). A variable or IER is safety critical if accuracy of information it passes is critical to safe operation of the BMDS or any element of the BMDS. The following general categories have been identified as safety critical:

- a. Any information which identifies a track as simulated or real.
- b. Any information which identifies that a BMDS element is participating in a specific event or activity (e.g., real world operations, test, or training).
- c. Any information which identifies that a specific BMDS element is participating in a flight test.
- d. Any information which identifies a track as a threat or non-threat.
- e. Any instructions or commands that could result in a change to war fighting posture of a BMDS element (e.g., a command to go to weapons free or weapons hold).
- f. Any instructions or commands to engage or to not engage a track.
- g. Any instructions or commands to terminate an engagement in progress.
- h. Any instructions or commands to the Sea Based X-Band Radar which would cause it to track an object.
- i. Any instructions or commands to an X-band radar which set or modify restrictions on radiating.
- j. Any instructions or commands to an interceptor intended to modify the trajectory so as to reduce collateral damage from launch debris.

3.14.9 Software Safety

The contractor's software system safety effort shall apply to all computer systems and subsystems that perform safety critical functions during assembly, handling, checkout, test, operation, maintenance, and disposal. In context of launch vehicle range safety, these systems and subsystems include auxiliary

support equipment (e.g., cranes and ground transport), vehicle GSE (e.g., fuel or oxidizer), and airborne systems.

In addition to developed safety critical computer systems and software, these requirements shall apply to all safety critical computer instructions and data residing on non-volatile memory devices, NDIs, COTS, and reused code.

Software identified as SCCSF shall be designed, developed, coded, tested, and maintained to meet requirements of [3.3](#) and [3.14.9.1](#).

3.14.9.1 Software Coding Standard and Requirements

In addition to requirements in ([3.3.2.3.2](#)), the contractor's software coding standard shall address:

- a. Execution Path: Contractors shall identify and document all paths to safety critical computing functions.
- b. Characteristics of Strong Data Typing: Safety critical functions and variables shall exhibit strong data characteristics, except in those cases where message formats are dictated by DOD standards. Safety critical functions and variables shall not employ a logic "1" and "0" to denote potentially hazardous states. Potentially hazardous states shall be represented by at least a unique five-bit pattern. Safe state shall be a pattern that cannot, as a result of a one, two, or three bit error, represent the potentially hazardous pattern. Potentially hazardous states shall also not be the inverse of the safe state. If a pattern other than these two unique codes is detected, software shall flag the error, revert to a safe state, and notify the operator. Decision statements in safety critical computing system functions shall not rely on inputs of all ones or all zeros.
- c. Critical Variable Identification: Models and code shall contain comments that note safety critical variables by describing the variable name, its properties, its unit values, and its use.
- d. Safety Critical Markings: Safety critical areas in product documentation, including source code, shall be uniquely marked or commented to support traceability IAW [3.2.10](#) and shall be written to support a clear and concise understanding of how safety requirements have been satisfied.

3.14.10 Software Maintenance Requirements for Safety Critical Computing Systems

The contractor shall implement these requirements when performing maintenance on safety critical computing system applications.

- a. Safety Critical Firmware Changes: Firmware changes in the field shall be issued as a fully functional and tested LRU. Product protection shall be IAW [3.12.5.2](#).
- b. Software Change Medium: Software installations in the field shall be issued as a complete executable on the appropriately controlled medium. Product protection shall be IAW [3.12.5.2](#).
- c. Modification Configuration Control: All modifications and updates shall be subject to strict configuration control ([3.3.3.11](#)).
- d. Maintenance Attributes: Documentation, comments, and modular architecture shall be IAW [3.3.2](#).

3.14.11 Design and Development of Computer Systems

For safety critical applications and computing systems, the contractor shall comply with the following requirements in addition to provisions [3.2](#), Design and Development, and [3.3](#), Software and Firmware. The contractor shall design and develop computer systems to meet requirements detailed in the following sections.

3.14.11.1 General Design Requirements

The contractor shall demonstrate by analysis and testing that computer systems meet the following requirements:

- a. A single software fault/output shall not cause a marginal or critical severity mishap.
- b. A combination of two software faults or outputs shall not cause a catastrophic severity mishap.

3.14.11.2 Design Verification and Validation

The Government and contractor shall support the Software Safety Working Group (SwSWG) in evaluating results from verification and validation of software throughout the design, development, and maintenance process to determine if safety design requirements are correctly and completely implemented. Test results shall be evaluated to identify potential safety anomalies.

3.14.11.3 System Design Requirements for Computer Systems

The contractors shall implement the following system design requirements in safety critical applications of computing systems.

3.14.11.3.1 Designed Safe States

The contractor's design shall have at least one safe state identified for each logistic and operational phase. This state shall be defined by the contractor and documented for review and approval by the cognizant MDA Program Office and MDA/QS.

3.14.11.3.2 Safe State Return

Contractors shall design computing systems to alert the operator, log relevant data, and provide the capability to recover hardware subsystems to a safe state when a computer system fault, a power fluctuation, or loss of power occurs, or when unsafe conditions are detected.

3.14.11.3.3 Safety Critical Data Isolation

The contractor shall design the system to preclude simulated data and TT&E event data from being inadvertently used in a safety critical process for which it was not intended.

- a. Messages shall be labeled so that simulated data does not appear to be real.
- b. The TT&E data shall be labeled as such.
- c. Applications shall not accept messages which are not consistent with the activity or mode the application is supporting.
- d. Safety critical activities such as operations and flight test shall be physically isolated from networks transmitting simulated or TT&E data which is not directly supporting safety critical activity. If physical isolation is not practical, the contractor shall use separate encryption keys to prevent data from being inadvertently used by an unintended application. Encryption shall be National Security Agency approved Type 1 or other forms of encryption conforming to the MDA Quality, Safety, and Mission Assurance Isolation Protection Profile (MDA-QS-IPP-001). All encryption schemes shall be reviewed and approved by MDA/QS before use.

3.14.11.3.4 Safety Critical Software Isolation

The contractor shall ensure that in operational systems, software which has not been tested and accepted for operational use shall not be executed on the same physical processor and/or memory device with safety critical software.

3.14.11.3.5 Input/Output Registers and Ports

The contractor's design for computer system input/output registers and ports shall not be used for both safety critical and non-safety critical functions unless the same safety design criteria are applied to non-critical functions.

3.14.11.3.6 Fault Detection

The contractor shall include a fault detection capability to detect, if possible, all hardware, software, and firmware failures or faults which render the system less than dual fault tolerant for catastrophic or single fault tolerant for critical severity hazards. The fault detection capability shall immediately alert the operator and provide the capability to recover the system to a safe state.

3.14.11.3.7 Circumvent Unsafe Conditions

The contractor's design shall not permit circumvention of detected unsafe conditions. If a battleshort condition is required in the system, it shall be designed such that it cannot be activated inadvertently.

3.14.11.3.8 Fallback and Recovery

The contractor's design shall include fallback and recovery to a designed safe state of reduced system functional capability in the event of a failure of system components.

3.14.11.3.9 Simulators

If simulated items, simulators, and test sets are required, the contractor shall design the system such that operational hardware cannot be inadvertently identified as a simulated item, simulator, or test set.

3.14.11.3.10 System Errors Log

The contractor's software shall make provisions for logging all detected system errors. The operator shall have the capability to review logged system errors. Errors in SCCSFs shall be alarmed and displayed to the operator immediately.

3.14.11.3.11 Positive Feedback Mechanisms

The contractor shall ensure software control of safety critical functions shall have feedback mechanisms that give positive indications of the functions occurrence.

3.14.11.3.12 Corruption of Computing Environment

The contractor's software design shall preclude an application from corrupting the underlying computing environment.

3.14.11.4 Power-Up System Initialization Requirements

The contractor shall design the system to power-up in a safe state. An initialization test shall be incorporated into the design that verifies the system is in a safe state and those safety critical circuits and components are tested to ensure their safe operation. The test shall also verify memory integrity and program load.

3.14.11.5 System Level Check

The contractor shall design computing systems to perform a system level check at power-up to verify the system is safe and functioning properly before executing safety critical functions or applying power to hardware controlled by the computing system. Periodic tests shall be performed by the software to monitor the state of the computing system.

3.14.11.6 Operational Checks

The contractor shall design the system to allow the operator of a BMDS component to conduct operational checks of testable safety features before establishing a link to other BMDS components.

3.14.11.7 Feedback Loops

The contractor shall ensure feedback loops from the system hardware are designed so software cannot cause a runaway condition due to failure of a feedback sensor.

3.14.11.8 Interface Control

The contractor's design shall ensure safety critical computing system functions and their interfaces to safety critical hardware are controlled at all times. The interface shall be monitored to ensure erroneous or spurious data does not adversely affect the system, interface failures are detected, and the state of the interface is safe during power-up, power fluctuations and interruptions, or in the event of system errors or hardware failures.

3.14.11.9 BMDS Interface Control

The contractor shall design the system such that interfaces between BMD Systems are monitored at all times to ensure data passed from one system to another is consistent with the event or activity the receiving system is supporting.

3.14.11.10 Inter-CPU Communications

The contractor shall design the system such that inter-CPU communications shall successfully pass verification checks in both CPUs before transfer of safety critical data. Periodic checks shall be performed to ensure interface integrity. Detected errors shall be logged. If the interface fails several consecutive transfers, the operator shall be alerted and transfer of safety critical data terminated until diagnostic checks can be performed.

3.14.11.11 Data Transfer Messages

The contractor shall design the system such that data transfer messages are of a predetermined format and content. Each transfer shall contain a word or character string indicating message length (if variable), type of data, and message content. As a minimum, parity checks and checksums shall be used for verification of correct data transfer. Where practical, Cyclic Redundancy Checks shall be used. No information from data transfer messages shall be used before verification of correct data transfer. Data messages shall contain an application mode that indicates intended purpose of the message (e.g., Operations, Training, Test, and Management). The contractor shall ensure message headers (labels) are bound to the message body. There shall be a mechanism used to detect and report cases in which the message header and body are separated.

3.14.11.12 External Functions

Contractors shall design safety critical functions so that two unique and distinct signals from separate processes are required for execution.

3.14.11.13 Value Verification

The contractor's software shall verify input values are within expected tolerance limits before executing safety critical functions. The software shall verify output values of safety critical variables before transmitting.

3.14.11.14 Full Scale Representations

The contractor's software shall accommodate and correctly process the full range of expected input values.

3.14.11.15 Safety Kernel

The contractor's design of safety kernels shall be:

- a. Resident in non-volatile read-only memory (ROM) or in protected memory that cannot be overwritten by the computing system.
- b. Designed and implemented so the safety kernel cannot be corrupted, misdirected, delayed, or inhibited by any other program in the system.
- c. Designed so a safety kernel failure will be detected and the system returned to a designed safe state.

3.14.11.16 Inadvertent Jumps

The contractor's design shall detect inadvertent jumps within, or into SCCSFs, return the system to a safe state, and, if practical, perform diagnostics and fault isolation to determine the cause of the inadvertent jump.

3.14.11.17 Overwritten Safety Critical Functions

The contractor's design shall ensure any safety critical functions overwritten by the loaded data/program triggers a warning message to the operator.

3.14.11.18 Safety Critical Computing System Functions User Interfaces

The contractor's design of user interface for computer systems executing SCCSFs shall meet design requirements of this section.

3.14.11.18.1 Processing Cancellation

The contractor shall design software so the operator may cancel current processing with a single action and have the system revert to a safe state.

3.14.11.18.2 Hazardous Function Initiation

The contractor's design shall ensure that two or more unique operator actions shall be required to initiate any potentially hazardous function or sequence of functions. The actions required shall be designed to minimize potential for inadvertent actuation and shall be checked for proper sequence.

3.14.11.18.3 Safety Critical Displays

The contractor shall ensure safety critical operator displays, legends, and other interface functions are clear, concise, and unambiguous and, where possible, use redundant display devices. Operator displays shall continually display the current operating mode (e.g., Test, Training, or Operations).

3.14.11.18.4 System Response to Operator Actions

The contractor shall ensure software is capable of detecting improper operator actions, alerting the operator, and preventing execution of safety critical functions. Alerts shall indicate the error and corrective action. The software shall also provide positive confirmation of valid data entry or actions taken (i.e., the software shall provide visual and aural feedback so the operator knows the software has accepted the action and is processing it). The system shall also provide a real time indication it is

functioning. Processing functions requiring several seconds or longer shall provide a status indicator to the operator during processing.

3.14.11.18.5 Safety Alerts

The contractor shall ensure safety critical alerts are readily distinguishable from all other alerts. The operator shall not be able to clear a safety critical alert without taking corrective action or performing required subsequent actions to complete the ongoing operation.

3.14.12 MDA Safety Integration

The Government and contractor shall comply with integration requirements in [3.14.12.1](#) and [3.14.12.2](#).

3.14.12.1 Integration Responsibility

Government and contractors with Integration responsibilities for safety functions shall:

- a. Perform safety risk assessments; analyze the integrated system design, operations, and specifically interfaces between products of each supplier and the end item; and summarize the mishap risk presented by the operation of the integrated system.
- b. Direct suppliers to perform subsystem safety analysis in support of the overall safety risk assessment.
- c. Resolve differences between suppliers in areas related to safety, especially during development of safety inputs to system and item specifications. Where the integrator cannot resolve problems, notify the cognizant MDA Program Office for resolution and action.
- d. Initiate action through the cognizant MDA Program Office to ensure information required by a Government or contractor from another contractor to accomplish safety tasks is provided.
- e. Establish and maintain a method of exchanging safety information among Government and contractor's organizations.
- f. Provide support to other MDA or external SSWGs.

3.14.12.2 Flow Down of Requirements from Contractor to Supplier

The contractor shall flow down the following requirements supplementing the supplier management requirements contained in [3.13](#):

- a. Suppliers shall maintain suitable documentation of safety analyses performed. These analyses shall be in formats that will permit incorporation of their data into the overall analysis program.
- b. Suppliers of safety critical items shall develop system safety program plans to be included as annexes to the contractor's SSPP.
- c. Suppliers shall provide information on software, component, and subassembly characteristics, including failure modes, failure rates, and possible hazards, which will permit the integrating Government or contractor to evaluate the items for their impact on system safety.
- d. Suppliers shall, when required, participate in the SSWG.

4.0 NOTES

4.1 Custodian

Requests for copies of this document should be submitted to:

Director
Quality, Safety, and Mission Assurance (QS)
Missile Defense Agency
Building 245
5700 18th Street
Fort Belvoir, VA 22060-5573

APPENDIX (A.1)

Mission Assurance Implementation Plan Development and Approval

APPENDIX (A.1)**Mission Assurance Implementation Plan Development and Approval****A.1.0 Introduction**

A Mission Assurance Implementation Plan (MAIP) defines a MDA Organization's implementation of the MAP with a level of detail sufficient to provide accountability and traceability.

Each MDA Organization not developing a Requirements Applicability Matrix described in Appendix A.2 shall develop a MAIP documenting applicability of each MAP section. The applicability shall include which requirement is applicable with rationale for exceptions; when in the BMDS acquisition lifecycle it is applicable; how the MAP requirement is implemented; and who is the implementing organization

A.1.1 Generate MAIP

Each MDA Organization shall develop a MAIP, which describes how the MAP will be implemented and how the MAP provisions are invoked (e.g., internal policy or instruction). The MAIP shall:

- a. Refer to each MAP section sequentially; describing what implementation methodology is used to accomplish MAP provisions along with rationale for exceptions or alternate approaches. Where existing, equivalent, documented procedures are in place, a simple reference to the procedure is sufficient.

Note: In some cases, an overarching procedure (e.g., Configuration Management) may cover an entire MAP provision (3.10) thus eliminating the need to spell out details at the section levels (3.10.1, 3.10.1.1, etc). Minor exceptions or clarifications, whether at the top level, or at section levels, should be addressed.

- b. Identify the executing organization for each applicable MAP section (e.g., MDA Organization, or other Government agency).
- c. Where applicable, provide need to phase the implementation (e.g., incrementally by block or contract), describe when in the BMDS acquisition lifecycle MAP provisions will be implemented and the rationale for such phasing.

The MAIP shall identify requirements performed and not performed and include rationale for exceptions or alternate approaches

A.1.2 MDA/QS MAIP Review

MDA/QS will work with each MDA Organization in parallel with MAIP development to resolve issues.

A.1.3 MDA MAIP Approval

The final MAIP will be jointly approved by the implementing organization's Director and the MDA/QS Director.

A.1.4 Conflict Resolution

Conflicts between the MAP and other requirements documents shall be resolved by MDA/QS, MDA Office of Primary Responsibility (e.g., DE, DT), and the cognizant MDA Program Office.

A.1.5 MAIP Implementation

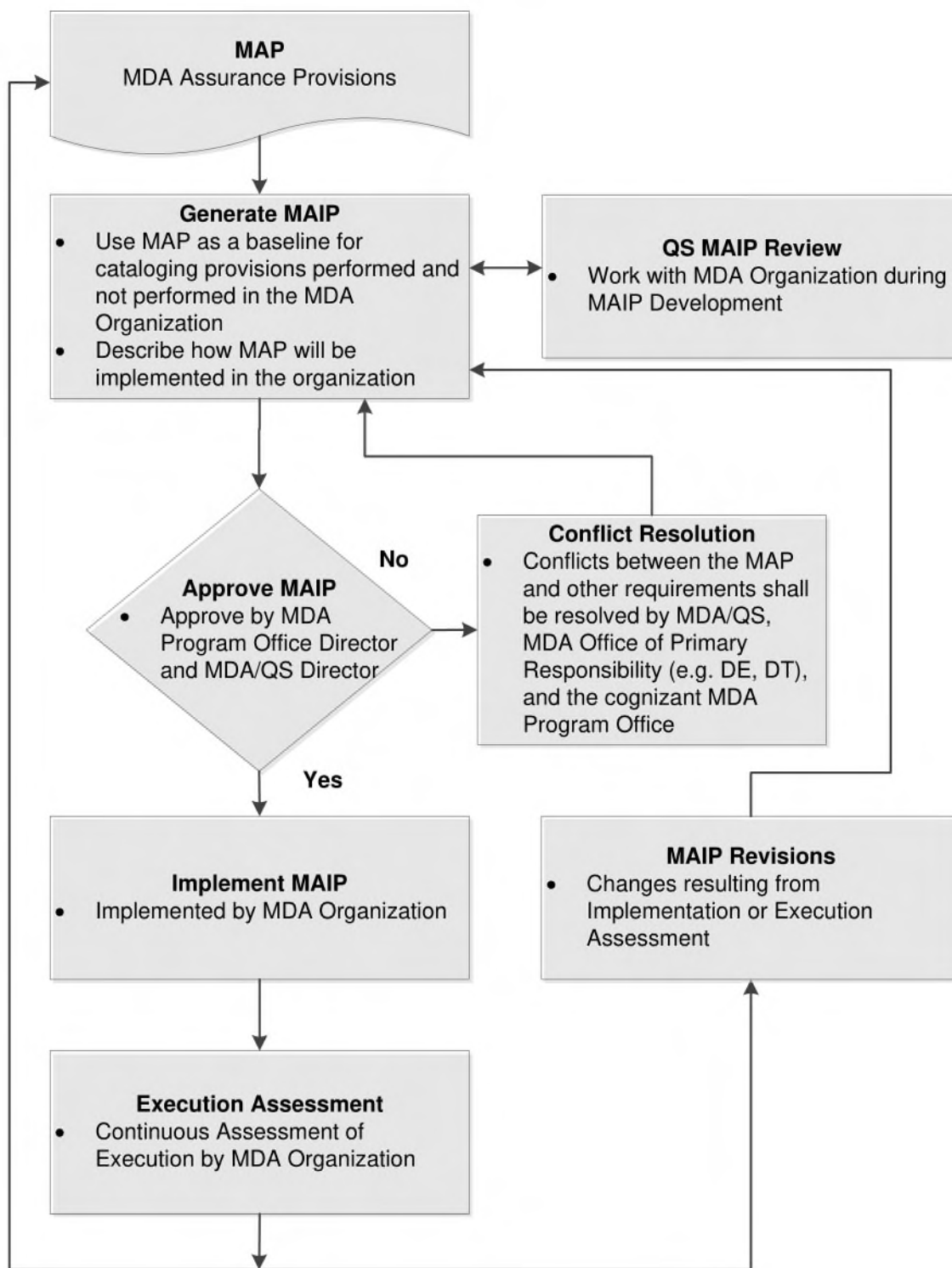
Each MDA Organization is accountable for implementation of their approved MAIP.

A.1.6 MAIP Revisions

Changes to the MAIP shall be reprocessed through the MAIP development, review, and approval processes.

A.1.7 Execution Assessment

Each MDA Organization shall periodically assess MAIP execution. As part of continuous improvement, the execution assessment results should be used to provide feedback and to improve the MAIP.

MAIP Development and Approval Flow

13 June 2014

MDA-QS-001-MAP-Rev B

APPENDIX (A.2)

Requirements Applicability Matrix

Date:

MDA-QS-001-MAP-REV B REQUIREMENTS APPLICABILITY MATRIX (RAM)



MDA Program/Product:

Distribution D: Distribution Authorized to the Department of Defense and U.S. DOD Contractors only for the purpose of contract performance, an arrangement requiring that this information be held in confidence, and that public distribution is restricted. Other requests shall be referred to MDA/DAC Contracting Office.

For Official Use Only Statement: This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the Freedom Of Information Act (5 U.S.C. Section 552). Exemption (3) & (5) applies.

Warning: This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. section 2751 et. seq.) or the Export Administration Act of 1979, as amended (50 U.S.C Appendix 2401 et. seq.) Violation of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DOD directive 5230.25

Destruction Statement: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

~~For Official Use Only~~

Approved by: _____

MIKE WADZINSKI

Director

Quality, Safety, and Mission Assurance (QS)

Approved by: _____

Director or Program Manager

MDA Program Office

Revision	Date	Description	Affected Pages

Table of Contents

DEFINITIONS	A-15
SCOPE.....	A-17
REQUIREMENTS	A-17
MDA-QS-001-MAP-Rev B, Requirements Applicability Matrix	A-19
RAM Development and Approval Flow	A-34
Subcontractor RAM Development and Approval Flow	A-35

DEFINITIONS**Applicability (APPL) Types**Yes (Y)

A (Y) in the applicability (Appl) column indicates the requirement is contractually applicable for this program as written in MAP (MDA-QS-001-MAP-REV B). Requirements indicated as applicable contain a note in the comment field of the matrix as follows:

(Y) MAP paragraph applies

No (N)

A (N) in the applicability column indicates that an exception has been taken to MAP requirements. The MAP requirement is not contractually applicable for this contract or purchase order. Requirements indicated as not applicable contain a note in the comment field of the matrix as follows:

(N) MAP paragraph does not apply because...{Include Brief Rationale}

Modified (M)

An (M) in the applicability column indicates the MAP requirement is applicable as modified for this contract or purchase order. Modifications include alternate approaches, and/or changes to MAP requirements. Modifications shall be incorporated in RAM comment field. Deleted text shall be shown as single lined-out text (e.g., ~~Xxxx-yyyy~~) and added text shall be shown as bold text (e.g., **Aaaaa bbbbbb**). Requirements which have been modified contain a note, along with the specific modified requirement, in the comment field of the matrix as follows:

(M) Replace MAP paragraph with:

"The contractor shall...{Include Modified Requirement Here}."

Integrated Digital Environment (IDE)Approval (A)

An (A) in the Comment column indicates a deliverable is to be submitted for approval.

Comments

Comments should be included in the matrix to provide additional information related to requirements applicability implementation and/or specific information on documentation submittals.

SCOPE

The Requirements Applicability Matrix (RAM), in conjunction with MDA-QS-001-MAP-REV B, MDA Assurance Provisions (MAP) specifies the Quality, Safety, and Mission Assurance (QSMA) requirements to be followed in development of products and services for this contract or purchase order. References to QSMA deliverables specified by these requirements are included in the RAM and List of Deliverables.

REQUIREMENTS

The Requirements Applicability Matrix herein tailors QSMA requirements contained in MDA-QS-001-MAP-REV B, for this MDA program/product and are applicable for this contract or purchase order. To the extent specified by this RAM, the contractor shall establish and maintain the necessary QSMA disciplines IAW MDA-QS-001-MAP REV B.

When subcontracts, statements of work, or purchase orders are made to safety and mission critical suppliers in support of this contract, statement of work, or purchase order, the contractor shall ensure appropriate QSMA requirements are flowed down utilizing Appendix A.2, Requirements Applicability Matrix contained in MDA-QS-001-MAP-REV B. The QSMA requirement flow down shall consider product(s)/service(s) mission criticality and phase. Subcontractor and Supplier RAMs shall be maintained to provide evidence of QSMA requirement flow down appropriateness. Subcontractor and Supplier RAMs shall be stored in IDE ([3.1.5](#)).

MDA-QS-001-MAP-Rev B, Requirements Applicability Matrix

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.1	Management		X	
3.1.1	Contract Reviews		X	
3.1.2	Management Reviews		X	
3.1.3	Technology Change Management			
3.1.4	Process Improvements and Core Metrics			
3.1.4.1	MDA Core Metrics			
3.1.5	Integrated Digital Environment			
3.1.6	Risk Management Program		X	
3.1.6.1	Risk Management Plan		X	(A) Risk Management Plan
3.1.7	Pedigree Program		X	
3.1.8	Internal Evaluation Program		X	
3.1.9	Training and Certification Program			
3.1.9.1	Training			
3.1.9.2	Certification			
3.1.10	Problem and Failure Reporting and Corrective Action System		X	
3.1.11	Data Exchange Programs Participation			
3.1.12	MDA Insight and Oversight			
3.1.12.1	MDA Assurance Representatives			
3.1.12.2	MDA Inspections			
3.1.12.3	MDA Evaluations			
3.1.13	Program Reviews			
3.1.14	Government Furnished Material, Equipment, or Information			
3.1.14.1	Contractor Acquired Property			
3.1.15	Repair, Refurbishment, and Modification		X	(A) Standards and procedures
3.1.16	Responsible Engineer			
3.2	Design and Development			
3.2.1	Integrated Product and Process Development			
3.2.2	Peer Reviews			
3.2.3	Technical Performance Measurement			
3.2.4	Systems Engineering for Design			
3.2.4.1	Element Systems Engineering Plan and Systems Engineering Management Plan		X	(A) SEP/SEMP
3.2.4.2	Contractor Systems Engineering Management Plan		X	(A) SEMP
3.2.5	Design for Interoperability			

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.2.6	Design for Producibility			
3.2.7	Design for Testability			
3.2.7.1	Testability Program Plan		X	(A) Testability Program Plan
3.2.8	Design for Supportability		X	(A) Life Cycle Sustainment Plan
3.2.9	Design for Commercial and Non-Developmental Items			
3.2.9.1	COTS/NDI Design Strategies			
3.2.10	Requirements Traceability and Verification Matrix			
3.2.11	System Design Verification and Validation			
3.2.12	Safety and Environmental Requirements			
3.2.13	Open Systems Design and Standards			
3.2.14	Modeling and Simulation			
3.2.14.1	Verification, Validation, and Accreditation Processes			
3.2.14.2	Models and Simulations Verification & Validation			
3.2.14.3	Models and Simulations Accreditation			
3.2.14.4	Accreditation Decision			
3.2.14.5	Verification, Validation, and Accreditation Documentation		X	(A) VV&A documentation
3.2.15	Classification of Characteristics			
3.2.15.1	Classification of Characteristics Levels			
3.2.16	Electromagnetic Environmental Effects Design & Verification			
3.2.17	Space Radiation, Nuclear Hardness and Survivability Program			
3.2.18	Transition to Operations or Production			
3.2.18.1	Transition to Production Plan		X	
3.2.19	Legacy Designs			
3.2.20	BMDS Technical Core Standards			
3.2.21	Safety and Mission Critical Computing Systems			
3.2.21.1	Computer System Synchronization			
3.2.21.2	Read-Only Memories			
3.2.21.3	Self-Checking Design Requirements			
3.2.21.3.1	Time Constraints for Execution			
3.2.21.3.2	Memory Checks			
3.2.21.4	Systems Degradation			

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.2.21.5	Unauthorized Interaction			
3.2.21.6	Unauthorized Access			
3.2.21.7	Peak Load Requirements			
3.2.21.8	Fault Tolerance			
3.3	Software and Firmware			
3.3.1	Management Processes			
3.3.1.1	Intergroup Coordination			
3.3.1.2	Software Development Plan		X	(A) Software Development Plan
3.3.1.3	Estimation			
3.3.1.4	Software and Firmware Risk Management			
3.3.1.5	Software Process Improvement			
3.3.1.6	Software and Firmware Supplier Management			
3.3.1.6.1	Flow Down of Requirements			
3.3.1.6.2	Acceptance of Supplier Software and Firmware Products			
3.3.1.7	Software Personnel Training			
3.3.2	Software Development, Maintenance, and Operational Processes			
3.3.2.1	Requirements		X	
3.3.2.1.1	Software Reuse		X	
3.3.2.2	Software Design		X	
3.3.2.3	Software Code/Implementation		X	
3.3.2.3.1	Software Programming Standards			
3.3.2.3.2	Software Coding Standards			
3.3.2.3.3	Software Code Analysis			
3.3.2.4	Software Test Coverage and Analysis			
3.3.2.4.1	Requirements Based Test Coverage Analysis			
3.3.2.4.2	Structural Test Coverage Analysis			
3.3.2.4.3	Software Threading and Concurrency Analysis			
3.3.2.4.4	Multitasking and Multicore Processing Analysis			
3.3.2.5	Software Unit Testing		X	
3.3.2.6	Software Integration Testing		X	
3.3.2.7	Software Qualification			
3.3.2.7.1	Software Qualification Test Report		X	
3.3.2.7.2	Software Requalification		X	
3.3.2.8	Regression Tests		X	
3.3.2.9	Software Test Program Status Reports		X	
3.3.2.10	System Integration		X	

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.3.2.11	System Qualification			
3.3.2.12	Software Installation		X	
3.3.2.12.1	Software Deliverable Package		X	(A) Software Deliverable Package
3.3.2.12.2	Software Release Review			
3.3.2.13	Software Acceptance			
3.3.2.14	Operation		X	
3.3.2.15	Software Maintenance		X	(A) Software Maintenance Plan
3.3.2.16	Software Retirement			
3.3.3	Supporting Activities and Processes			
3.3.3.1	Software Quality Assurance Plan		X	(A) Software Quality Assurance Plan and subsequent updates
3.3.3.2	Software Verification		X	
3.3.3.3	Software Validation		X	
3.3.3.4	Support of Independent Verification and Validation			
3.3.3.5	Independent Verification and Validation			
3.3.3.6	Software Reviews		X	
3.3.3.7	Software Audits		X	
3.3.3.8	Software Problem Reporting		X	
3.3.3.9	Software Dependability			
3.3.3.9.1	Software Reliability Program			
3.3.3.9.1.1	Software Reliability Program Plan (SRPP)		X	(A) SRPP. Unless integrated in RM&A Plan (3.5.1)
3.3.3.9.1.2	Software Reliability Documentation		X	
3.3.3.9.1.3	Allocation of Reliability Requirements to Software			
3.3.3.9.1.4	Software Reliability Analysis		X	
3.3.3.9.1.5	Software Reliability Evaluation and Achievement		X	
3.3.3.9.1.6	Fault Avoidance and Fault Tolerance			
3.3.3.10	Software Safety			
3.3.3.11	Software and Firmware Configuration Management			
3.3.3.11.1	Software Configuration Items			
3.3.3.11.2	Software and Firmware Change Control Process			
3.3.3.11.3	Software Library			
3.3.3.11.4	Software Configuration Audits		X	
3.3.3.11.5	Software Status Accounting		X	
3.3.3.11.6	Software and Firmware Media Generation		X	
3.3.3.12	Software Documentation			
3.3.4	Firmware Development Plan		X	(A) Firmware Development Plan
3.4	Technical and Mission Assurance Reviews			
3.4.1	Technical Reviews		X	
3.4.1.1	Initial Technical Review			
3.4.1.2	Alternative Systems Review			

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.4.1.3	Systems Requirements Review			
3.4.1.4	System Functional Review			
3.4.1.5	Software Specification Review			
3.4.1.6	Preliminary Design Assessments/Critical Design Assessments			
3.4.1.7	Preliminary Design Review			
3.4.1.8	Critical Design Review			
3.4.1.9	Test Readiness Review			
3.4.1.9.1	MDA Executive Level Test Reviews			
3.4.1.10	System Verification Review			
3.4.1.11	Functional Configuration Audit			
3.4.1.12	Production Readiness Review			
3.4.1.12.1	Follow-On Production Readiness Review			
3.4.1.13	Physical Configuration Audit			
3.4.2	Mission Assurance Reviews		X	
3.4.2.1	Mission Readiness Review			
3.4.2.2	Pre-Environmental Review			
3.4.2.3	Pre-Shipment Review			
3.4.2.4	Mission Operations Review			
3.4.2.5	Flight Operations Review			
3.4.2.6	Pre-Flight Readiness Review			
3.4.2.7	Launch Readiness Review			
3.5	Reliability, Maintainability, and Availability			
3.5.1	Reliability, Maintainability, and Availability Program Plan		X	(A) RM&A Program Plan
3.5.1.1	Reliability, Maintainability, and Availability Program Planning			
3.5.2	Supplier Reliability, Maintainability, and Availability Requirements		X	
3.5.3	Failure Reporting, Analysis, and Corrective Action System		X	
3.5.4	Failure Review Board			
3.5.4.1	Unverified Failures		X	(A) Policy or Procedure
3.5.5	Reliability Modeling, Allocation, and Prediction			
3.5.5.1	Reliability Prediction Methodology			
3.5.6	Reliability Analyses			
3.5.6.1	Failure Modes, Effects, and Criticality Analysis		X	(A) FMECA report
3.5.6.2	Fault Tree Analysis		X	
3.5.6.3	Finite Element Analysis		X	
3.5.6.4	Sneak Circuit Analysis		X	
3.5.6.5	Worst Case Analysis		X	
3.5.6.6	Electrical, Mechanical, and Thermal Stress Analyses			

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.5.6.6.1	Thermal Stress Analysis		X	
3.5.6.6.2	Mechanical Stress Analysis		X	
3.5.6.6.3	Electrical/Electronic Stress Analysis		X	
3.5.7	Mission Critical Items		X	
3.5.8	Effects of Functional Testing, Storage, Handling, Packaging, Transportation, and Maintenance			
3.5.9	Controlled and Limited Life Items			
3.5.10	Reliability Growth Test Program			
3.5.11	Accelerated Life Testing		X	
3.5.12	Highly Accelerated Life Test			
3.5.13	Highly Accelerated Stress Screen			
3.5.14	Process Failure Modes and Effects Analysis		X	
3.5.15	Environmental Stress Screening			
3.5.16	Reliability Qualification Test Program/Demonstration		X	
3.5.17	Maintainability Modeling, Allocations, and Predictions			
3.5.18	Maintainability Analysis			
3.5.19	Maintainability Demonstration		X	
3.5.20	Availability Modeling, Allocations, and Predictions			
3.5.21	Availability Assessment			
3.5.22	Reliability, Maintainability, and Availability of Government Furnished Equipment/ Information			
3.5.23	Reliability Surveillance of Deployed and Fielded Systems		X	(A) Methodology for Determining Deployed and Fielded Systems Reliability
3.6	Parts, Materials, and Processes Control Program			
3.6.1	Parts, Materials, and Processes Plan		X	Parts, Materials, and Processes Plan
3.7	Integrated Test and Evaluation Program		X	
3.7.1	Integrated Test and Evaluation Program Plan		X	(A) Integrated Test and Evaluation Program Plan
3.7.2	Engineering Evaluation Tests		X	
3.7.2.1	Integration Tests			
3.7.2.2	Interoperability Tests			
3.7.2.3	Test-Like-You-Fly			
3.7.3	Qualification and Requalification Test Program		X	(A) Requalification decision
3.7.3.1	Qualification Program Plan		X	(A) Qualification Program Plan

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.7.3.2	Qualification Tests		X	(A) Test Plans and Reports
3.7.3.2.1	Qualification by Similarity		X	(A) Decisions to qualify based on similarity
3.7.4	Acceptance Tests		X	
3.7.5	Production Assessment Tests		X	
3.7.6	Surveillance and Service Life Evaluation Tests		X	
3.7.6.1	Surveillance and Service Life Evaluation Test Program Plan		X	
3.7.7	Ground and Flight Tests		X	(A) Test Plans and Procedures (A) Test Report
3.7.7.1	Test Risk Management Program			
3.7.7.2	Critical Test Gate Process			
3.7.7.3	Post-Test Performance Analysis		X	
3.7.7.4	Failure Review Process		X	(A) Flight failure corrective action
3.7.8	Modeling and Simulation			
3.7.9	Test Plans			
3.7.10	Test Procedures			
3.7.11	Test Reports			
3.8	Test, Measuring, and Diagnostic Equipment and Standards			
3.8.1	Selection and Design		X	(A) Review and Approval of Variances
3.8.1.1	Test, Measuring, and Diagnostic Equipment Configuration Documentation			
3.8.1.2	Evaluation of Test, Measuring, and Diagnostic Equipment		X	
3.8.1.3	Proofing, Qualification, and Correlation		X	
3.8.2	Calibration and Maintenance			
3.8.2.1	Calibration and Maintenance Procedures		X	
3.8.2.2	Records and Analysis		X	
3.8.2.3	Out-of-Tolerance Conditions			
3.8.2.4	Calibration Standards and Reference Materials		X	(A) Request for Review and Approval of Variances
3.8.3	General Test, Measuring, and Diagnostic Equipment and Standards Requirements		X	
3.8.3.1	Intervals and Recall		X	
3.8.3.2	Labeling			
3.8.3.3	Sealing for Integrity			
3.8.3.4	Removal of Test, Measuring, and Diagnostic Equipment and Standards			
3.8.3.5	Test Station Logs			
3.9	Interface Management			
3.9.1	Interface Control Plan		X	

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.9.1.1	Interface Control Plan Development			
3.9.2	Interface Documentation		X	(A) Interface documentation
3.9.3	Interface Control Working Groups		X	
3.9.4	Interface Change Notice		X	
3.10	Configuration Management			
3.10.1	Configuration Management Plan		X	(A) Configuration Management Plan
3.10.2	Supplier Configuration Management			
3.10.3	Configuration Identification			
3.10.3.1	Product Information			
3.10.3.2	Product Structure and Configuration Item Selection		X	(A) List of Configuration Item candidates
3.10.3.3	Product Identifiers			
3.10.3.3.1	Unique Software Identifiers			
3.10.3.3.2	Identifying Individual Units of Product			
3.10.3.3.3	Identifying Groups of Units of a Product			
3.10.3.3.4	Department Of Defense Item Unique Identification			
3.10.3.4	Document Identification			
3.10.3.5	Configuration Baselines			
3.10.3.5.1	Establishing Configuration Baselines			
3.10.3.5.2	Types of Configuration Baselines			
3.10.3.6	Interface Control			
3.10.4	Configuration Change Management			
3.10.4.1	Classifying Changes		X	(A) Approval by MDA for Major changes (A) Approval by MDA for minor changes if stipulated by contract
3.10.4.1.1	Class I Engineering Change			
3.10.4.2	Documenting Requests for Engineering Changes			
3.10.4.3	Configuration Control Board		X	
3.10.4.4	Change Effectivity Determination			
3.10.4.5	Change Implementation and Verification			
3.10.4.6	Change Management Process Applied to Variances		X	
3.10.4.6.1	Requests for Waiver		X	
3.10.4.6.2	Requests for Deviation		X	
3.10.4.6.2.1	Restrictions on Waivers and Deviations			
3.10.4.6.2.2	Classification of Waivers and Deviations			

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.10.4.6.3	Review and Approval of Waivers and Deviations		X	(A) Critical or Major variance requests approved by MDA (A) Minor variance requests approved by MDA
3.10.5	Configuration Status Accounting		X	
3.10.6	Configuration Audit			
3.10.7	Configuration Management of Digital Data			
3.10.7.1	Digital Data Identification			
3.10.7.2	Data Status Level Management			
3.10.7.3	Digital Data Transmittal			
3.10.7.4	Data Access Control			
3.11	Control of Nonconforming Items and Materials			
3.11.1	Preliminary Review			
3.11.2	Material Review Board			
3.11.2.1	Material Review Board Membership			
3.11.2.2	Material Review Board Dispositions		X	
3.12	Fabrication and Quality		X	
3.12.1	Manufacturing, Process, and Quality Control Planning		X	
3.12.2	Process Selection and Development			
3.12.2.1	Process Selection and Development Planning			
3.12.2.2	Mission Critical Process Selection			
3.12.2.3	Special Processes			
3.12.3	Product Test and Inspection Plan		X	
3.12.4	Fabrication and Quality Procedures			
3.12.4.1	Fabrication and Process Procedures			
3.12.4.2	Test and Inspection Procedures		X	(A) Acceptance test and inspection procedures
3.12.4.3	Workmanship Standards		X	(A) Alternate standards
3.12.4.3.1	Connector Mating and Demating			
3.12.4.3.2	Threaded Fasteners and Torque			
3.12.5	Product Control during Fabrication			
3.12.5.1	Product Identification and Handling			
3.12.5.2	Product Protection			
3.12.5.2.1	Electrostatic Discharge Controls		X	

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.12.5.2.2	Contamination Control Program		X	
3.12.5.2.2.1	Clean Rooms			
3.12.5.2.3	Foreign Object Elimination Program		X	
3.12.5.3	Product Status Indication		X	
3.12.6	Fabrication Process Control			
3.12.6.1	Process Qualification and Requalification Program		X	
3.12.6.2	Fabrication and Quality Metrics			
3.12.6.3	Fabrication Defects		X	
3.12.6.4	Continuous Process Improvement			
3.12.7	Fabrication Environmental Stress Screening		X	
3.12.8	Fabrication Quality Verification			
3.12.8.1	In-Process and Acceptance Test and Inspection		X	(A) Procedures for tests and inspections
3.12.8.2	First Article Test and Inspection		X	
3.12.8.3	Nondestructive Test and Inspection		X	
3.12.8.4	Nonconforming Items Control			
3.12.9	Fabrication and Quality Records		X	
3.12.9.1	Fabrication Records			
3.12.9.2	Quality Control Records			
3.12.9.2.1	Closeout Photographs		X	
3.12.10	Packaging, Handling, Storage, and Transportation of Product			
3.12.10.1	Packaging			
3.12.10.2	Handling and Storage			
3.12.10.3	Preparation for Shipment and Transportation			
3.12.11	Lifting Devices and Equipment Program			
3.12.11.1	Identification of Critical Lifts		X	
3.12.11.2	Lifting Devices and Equipment Program Certification		X	(A) Alternate inspection, testing, and certification methods
3.12.11.3	Identification of Critical Moves			
3.13	Supplier Management			
3.13.1	Supplier Selection		X	
3.13.1.1	Safety and Mission Critical Supplier List		X	
3.13.1.2	Conditional Source Approval			
3.13.2	Supplier Ratings			
3.13.3	Supplier Evaluations		X	
3.13.4	Supplier Program Requirements		X	
3.13.4.1	Supplier Management System		X	
3.13.5	Procurement Process			

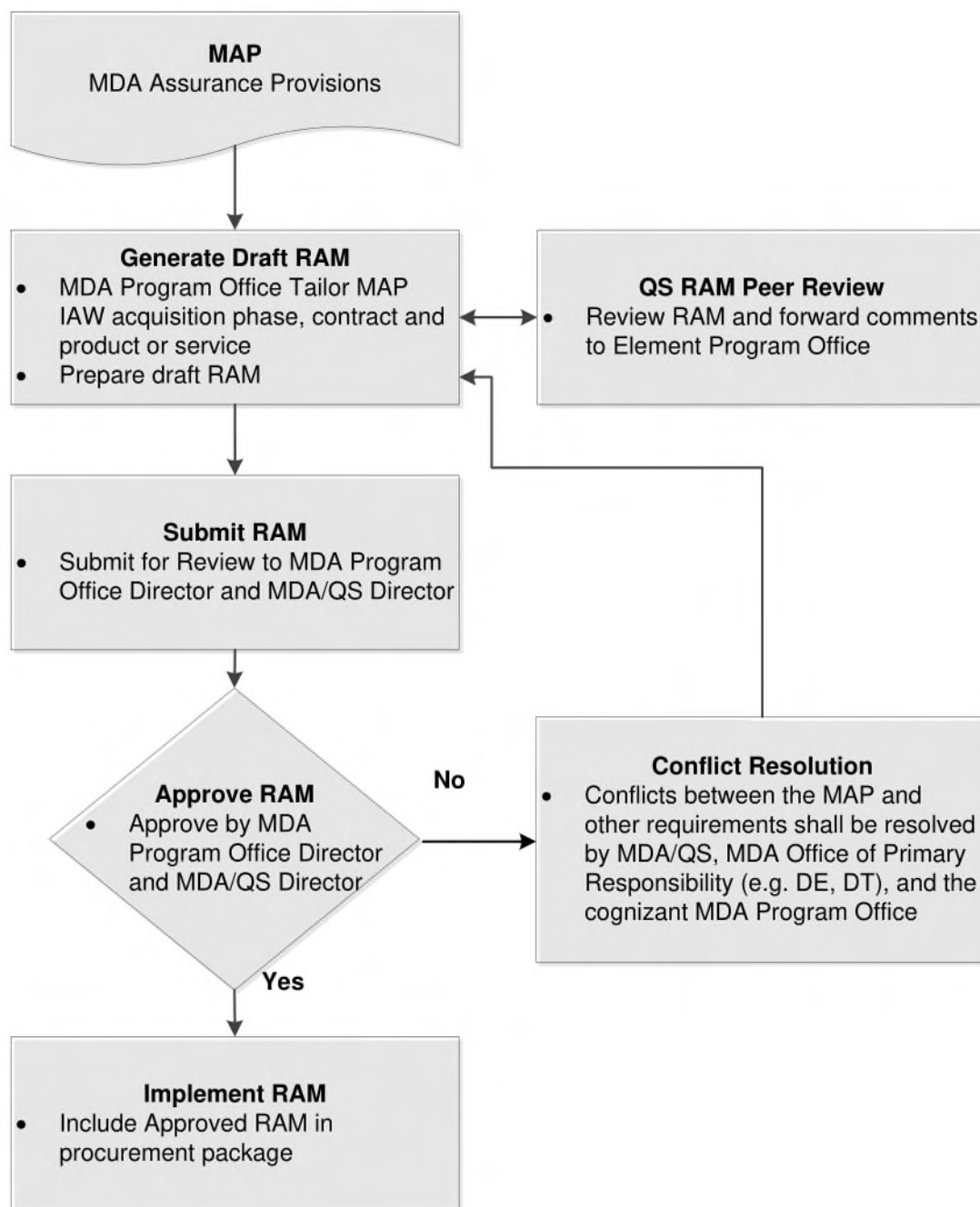
Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.13.5.1	Technical Requirements			
3.13.5.2	Detailed Provisions			
3.13.5.3	Procurement Document Review			
3.13.5.4	Procurement Document Change Control			
3.13.6	Control of Customer/Government Furnished Material			
3.13.7	Government Source Inspection			
3.13.8	Contractor Source Inspection			
3.13.9	Receiving Inspection and Test			
3.13.10	Intra-Corporate Work Transfers			
3.14	SAFETY			
3.14.1	Safety Program Requirements			
3.14.1.1	Safety Policies			
3.14.1.2	Safety Task Documentation			
3.14.1.2.1	System Safety Program Plan		X	(A) System Safety Program Plan
3.14.1.2.2	System Safety Hazard Analysis and Report		X	
3.14.1.2.3	Safety Assessment Report			
3.14.1.2.4	Safety Variance (Waiver/Deviation) Reporting		X	
3.14.1.2.5	Engineering Change Proposal System Safety Reports		X	(A) Hazard Analysis Reports and/or Safety Assessment Reports associated with ECPs and variances
3.14.1.2.6	Integrated System Safety Program Plan		X	(A) Integrated System Safety Program Plan
3.14.1.2.7	Health Hazard Assessment Report		X	
3.14.1.2.8	Safety Incident/Near Miss Report		X	
3.14.1.2.9	Management Trends Reports		X	
3.14.1.2.10	Message Modification Technologies Reporting and Approval			
3.14.1.3	System Safety Working Groups			
3.14.1.4	Hazard Tracking			
3.14.1.5	Safety Verification		X	
3.14.1.6	Safety Defect/Deficiency Assessment		X	
3.14.1.7	System Safety Program Reviews/Audits		X	
3.14.2	System Safety Requirements		X	(A) Safety documentation
3.14.3	System Safety Engineering Approach			
3.14.3.1	System Safety Hazard Identification and Analysis Methodology			

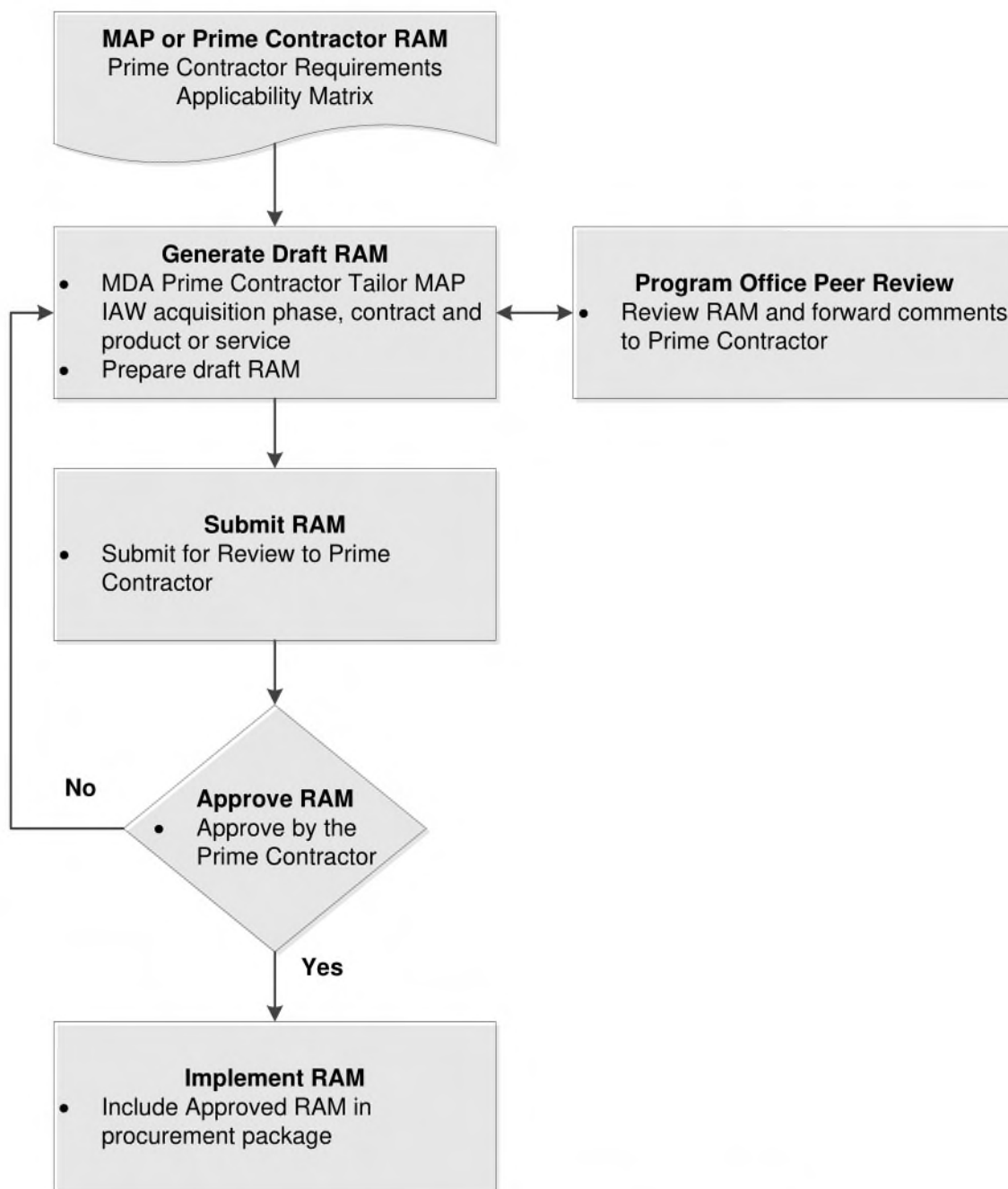
Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.14.3.2	Assessment of Mishap Risk			
3.14.3.3	Risk Acceptance Authority			
3.14.3.4	Mishap Investigations		X	
3.14.4	Safety Design Criteria			
3.14.4.1	Unacceptable Conditions			
3.14.4.2	Design Constraints			
3.14.4.3	Interlock Status and Restoration			
3.14.4.4	Ignition System Safety Requirements			
3.14.4.5	Fuze System Safety Requirements			
3.14.4.6	Hazardous Materials Transportation			
3.14.4.7	Insensitive Munitions Design and Safety Tests			
3.14.4.8	Ordnance Systems			
3.14.4.9	Missile and Space Vehicle Pressure Systems			
3.14.4.10	Orbital Debris			
3.14.5	Safety and Health			
3.14.5.1	Occupational Safety and Health		X	
3.14.5.1.1	Hazardous Materials Management		X	
3.14.5.1.2	Human Engineering		X	
3.14.5.1.3	Lasers			
3.14.5.1.4	Human Exposure to Radio Frequency			
3.14.6	Test and Range Safety			
3.14.6.1	Test Safety		X	
3.14.6.2	Range Safety			
3.14.6.2.1	Flight Termination System and Range Safety Tracking System Standards			
3.14.6.2.2	Three-Tone Receivers			
3.14.6.2.3	FTS Receiver Implementation Exclusivity			
3.14.6.2.4	Flight Safety Analysis		X	
3.14.7	Safety Critical Computing System Functions		X	
3.14.8	Safety Critical Variables and Information Exchange Requirements			
3.14.9	Software Safety			
3.14.9.1	Software Coding Standard and Requirements			
3.14.10	Software Maintenance Requirements for Safety Critical Computing Systems			
3.14.11	Design and Development of Computer Systems			

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
3.14.11.1	General Design Requirements			
3.14.11.2	Design Verification and Validation			
3.14.11.3	System Design Requirements for Computer Systems			
3.14.11.3.1	Designed Safe States			
3.14.11.3.2	Safe State Return			
3.14.11.3.3	Safety Critical Data Isolation			
3.14.11.3.4	Safety Critical Software Isolation			
3.14.11.3.5	Input/Output Registers and Ports			
3.14.11.3.6	Fault Detection			
3.14.11.3.7	Circumvent Unsafe Conditions			
3.14.11.3.8	Fallback and Recovery			
3.14.11.3.9	Simulators			
3.14.11.3.10	System Errors Log			
3.14.11.3.11	Positive Feedback Mechanisms			
3.14.11.3.12	Corruption of Computing Environment			
3.14.11.4	Power-Up System Initialization Requirements			
3.14.11.5	System Level Check			
3.14.11.6	Operational Checks			
3.14.11.7	Feedback Loops			
3.14.11.8	Interface Control			
3.14.11.9	BMDs Interface Control			
3.14.11.10	Inter-CPU Communications			
3.14.11.11	Data Transfer Messages			
3.14.11.12	External Functions			
3.14.11.13	Value Verification			
3.14.11.14	Full Scale Representations			
3.14.11.15	Safety Kernel			
3.14.11.16	Inadvertent Jumps			
3.14.11.17	Overwritten Safety Critical Functions			
3.14.11.18	Safety Critical Computing System Functions User Interfaces			
3.14.11.18.1	Processing Cancellation			
3.14.11.18.2	Hazardous Function Initiation			
3.14.11.18.3	Safety Critical Displays			
3.14.11.18.4	System Response to Operator Actions			
3.14.11.18.5	Safety Alerts			
3.14.12	MDA Safety Integration			
3.14.12.1	Integration Responsibility			
3.14.12.2	Flow Down of Requirements from Contractor to Supplier			
Appendix B – MDA Core Metrics				

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
B.4.4.1	Software Schedule Performance			
B.4.4.2	Software Development Progress			
B.4.4.3	Sprint Progress			
B.4.4.4	On-Time Delivery of Software Products			
B.4.4.5	Software Earned Schedule			
B.4.4.6	Schedule Performance Index and Schedule Variance			
B.4.4.7	Functionality and Milestone Progress			
B.4.4.8	Software Schedule Compression			
B.4.4.9	Software Unit Testing Progress			
B.4.4.10	Test and Integration Progress			
B.4.5.1	Cost Performance Index and Cost Variance			
B.4.5.2	Supplier Latest Revised Estimate			
B.4.5.3	Staffing Adequacy			
B.4.5.4	Software Cost Performance			
B.4.5.5	Software Staffing			
B.4.5.6	Software Staffing Profile			
B.4.6.1	Requirements Volatility Index			
B.4.6.2	Software Requirements Stability			
B.4.6.3	Software Size Estimate			
B.4.6.4	Software Interface Stability			
B.4.6.5	Software Functionality Stability			
B.4.6.6	Software Coding Progress			
B.4.7.1	Defect Density			
B.4.7.2	Defect Profile			
B.4.7.3	Defect Closure			
B.4.7.4	Defect Containment			
B.4.7.5	First Time Quality of Software			
B.4.7.6	Defect History			
B.4.7.7	Engineering Change Proposal Cycle Time			
B.4.7.8	Engineering Change Proposal Approval Rate			
B.4.7.9	Number of Deviation Requests and Percent Recurring			
B.4.7.10	Change Incorporation Rate			
B.4.7.11	Completion of Class I Engineering Change Proposals Implementing Actions			
B.4.7.12	Rework			

Paragraph Number	Title	Appl (Y/N/M)	IDE	Comment
B.4.7.13	Failure Review Board			
B.4.7.14	Foreign Object Elimination			
B.4.7.15	Waivers and Deviations			
B.4.7.16	MRB Actions, Dispositions, and Cost Metrics			
B.4.7.17	Occupational Safety			
B.4.7.18	System Safety Progress			
B.4.7.19	Software Safety Status			
B.4.7.20	Inherent Availability			
B.4.7.21	Operational Availability			
B.4.7.22	Mean Time To Repair			
B.4.7.23	Mean Time To Restore Functions			
B.4.7.24	Inherent Mean Time Between Critical Failure			
B.4.7.25	Operational Mean Time Between Critical Failures			
B.4.7.26	Mean Logistics Delay Time			
B.4.7.27	Mean Repair Time			
B.4.7.28	Fault Detection			
B.4.7.29	Fault Isolation			
B.4.7.30	Maintenance Ratio			
B.4.8.1	Software Productivity			
B.4.8.2	Software Requirements Ambiguity			
B.4.8.3	Software Requirements Incompleteness			
B.4.8.4	Software Reuse Profile			
B.4.8.5	Programming Languages Profile			
B.4.8.6	Resource Utilization			
B.4.8.7	Cyclomatic Complexity			
Appendix C – Workmanship Requirements				
C.1	Workmanship Standard Criteria			
C.2	Connector Mating and Demating			
C.3	General Torque Requirements			

RAM Development and Approval Flow

Subcontractor RAM Development and Approval Flow

Note: This process shall be followed for all levels of the supply chain.

APPENDIX (B)

MDA Core Metrics

13 June 2014

MDA-QS-001-MAP-Rev B

Table of Contents

B.1	Introduction	B-7
B.2	Metrics Overview.....	B-7
B.3	Definition of Terms	B-7
B.4	Roles and Responsibilities for Metrics Program Implementation	B-7
B.4.1	Metrics Analysis Process.....	B-7
B.4.1.1	Evaluation of Individual Metrics and Determination of Associated Status Condition...	B-7
B.4.2	MDA Core Metrics Report.....	B-9
B.4.3	Metrics Indicators	B-11
B.4.4	Schedule and Progress	B-12
B.4.4.1	Software Schedule Performance.....	B-13
B.4.4.2	Software Development Progress.....	B-15
B.4.4.3	Sprint Progress	B-17
B.4.4.4	On-Time Delivery of Software Products	B-19
B.4.4.5	Software Earned Schedule.....	B-21
B.4.4.6	Schedule Performance Index and Schedule Variance	B-23
B.4.4.7	Functionality and Milestone Progress	B-25
B.4.4.8	Software Schedule Compression	B-27
B.4.4.9	Software Unit Testing Progress.....	B-29
B.4.4.10	Test and Integration Progress	B-31
B.4.5	Cost and Resources	B-33
B.4.5.1	Cost Performance Index and Cost Variance	B-34
B.4.5.2	Supplier Latest Revised Estimate	B-36
B.4.5.3	Staffing Adequacy.....	B-38
B.4.5.4	Software Cost Performance	B-41
B.4.5.5	Software Staffing.....	B-43
B.4.5.6	Software Staffing Profile	B-45

B.4.6	Growth and Stability	B-47
B.4.6.1	Requirements Volatility Index.....	B-48
B.4.6.2	Software Requirements Stability	B-50
B.4.6.3	Software Size Estimate.....	B-52
B.4.6.4	Software Interface Stability	B-54
B.4.6.5	Software Functionality Stability.....	B-56
B.4.6.6	Software Coding Progress	B-58
B.4.7	Adequacy, Quality, Safety, and Performance	B-60
B.4.7.1	Defect Density	B-62
B.4.7.2	Defect Profile	B-64
B.4.7.3	Defect Closure	B-66
B.4.7.4	Defect Containment	B-68
B.4.7.5	First Time Quality of Software	B-70
B.4.7.6	Defect History.....	B-72
B.4.7.7	Engineering Change Proposal Cycle Time.....	B-75
B.4.7.8	Engineering Change Proposal Approval Rate	B-78
B.4.7.9	Number of Deviation Requests and Percent Recurring.....	B-80
B.4.7.10	Change Incorporation Rate	B-82
B.4.7.11	Completion of Class I Engineering Change Proposals Implementing Actions.....	B-84
B.4.7.12	Rework	B-86
B.4.7.13	Failure Review Board.....	B-88
B.4.7.14	Foreign Object Elimination	B-90
B.4.7.15	Waivers and Deviations.....	B-92
B.4.7.16	Material Review Board Actions, Dispositions, and Cost Metrics.....	B-95
B.4.7.17	Occupational Safety.....	B-97
B.4.7.18	System Safety Progress	B-99
B.4.7.19	Software Safety Status	B-101
B.4.7.20	Inherent Availability	B-103

B.4.7.21	Operational Availability	B-105
B.4.7.22	Mean Time To Repair	B-107
B.4.7.23	Mean Time To Restore Function.....	B-109
B.4.7.24	Inherent Mean Time Between Critical Failure	B-111
B.4.7.25	Operational Mean Time Between Critical Failure.....	B-113
B.4.7.26	Mean Logistics Delay Time	B-115
B.4.7.27	Mean Repair Time	B-117
B.4.7.28	Fault Detection	B-119
B.4.7.29	Fault Isolation	B-121
B.4.7.30	Maintenance Ratio	B-123
B.4.8	Software Development Environment	B-125
B.4.8.1	Software Productivity	B-126
B.4.8.2	Software Requirements Ambiguity	B-128
B.4.8.3	Software Requirements Incompleteness.....	B-130
B.4.8.4	Software Reuse Profile	B-132
B.4.8.5	Programming Languages Profile.....	B-134
B.4.8.6	Resource Utilization.....	B-136
B.4.8.7	Cyclomatic Complexity.....	B-138

13 June 2014

MDA-QS-001-MAP-Rev B

B.1 Introduction

The MDA Core Metrics Program consists of a comprehensive set of metrics that provides valuable insight into process performance, and product quality, status, trends, and risks.

Contractors are required to develop and sustain a system for collection, analysis, and reporting of metrics for management information needs.

In addition to implementing metrics defined in this Appendix, contractors may continue to use existing metrics and implement new metrics to meet emerging information needs.

B.2 Metrics Overview

A metric per IEEE 610.12 is defined as “a quantitative measure of the degree to which a system, component, or process possesses a given attribute.” Timely, complete, and consistent metrics reporting promotes effective communication of performance and quality to MDA leadership and stakeholders.

B.3 Definition of Terms

Performance Levels: Information that places or positions the organization's progress toward its desired outcome on a meaningful measurement scale. Performance levels permit evaluation relative to past performance, projections to support goals, and appropriate comparisons.

Performance Trends: The term “trends” refers to information that indicates direction and rate of change of levels. Trends provide a time sequence of organizational performance toward achieving corresponding desired outcome. Generally accepted statistical sampling techniques will determine minimum sample size needed to ascertain the trend.

Comparative/Benchmark Information: Comparative information enables direct comparison of the organization's performance to performance on similar programs/projects or performance by best-in-class organizations with regard to the similar performance indicator.

Corrective Action Plan: The term “corrective action plan” (3.1.10) refers to specific corrective actions that are needed to implement short-and-longer term performance improvements. Corrective action plans include details of resource commitments, actions, and milestones for accomplishing specific objectives.

B.4 Roles and Responsibilities for Metrics Program Implementation

MDA Program Offices and contractor managers are responsible to leverage metrics data, information, and reports in their decision making process. Metrics status and interpretation shall be reviewed in staff meetings, off-site reviews, program reviews, corporate boards, and other status meetings as appropriate.

Contractors shall collect data necessary to comply with values required in metrics specifications. Contractors shall perform analysis and interpretation of metrics data and report results to the appropriate level of management for review and corrective action as needed. This data and reports, including interpretation, shall be forwarded to the cognizant MDA Program Office no later than two weeks (10 working days) after the end of the monthly reporting period.

B.4.1 Metrics Analysis Process

B.4.1.1 Evaluation of Individual Metrics and Determination of Associated Status Condition

Each reported metric is evaluated, and its associated Status Condition is rated “Red”, “Yellow”, or “Green” in accordance with the following criteria and expert opinion of the analyst performing the metric evaluation:

Red Status Condition: Indicates a serious risk or problem which is or is likely to become outside the control of the MDA Program Office or a serious risk or problem that is either lacking a mitigation or consequence corrective action plan or such a plan is not being actively managed.

Yellow Status Condition: Indicates a potential or actual serious risk or problem which is within control of the Program Office and for which a mitigation or consequence corrective action plan exists and is being actively managed.

Green Status Condition: Indicates absence of conditions which would establish a "Red" or "Yellow" condition.

MDA metrics analysis is transitioning to a process based in Statistical Process Control. Accordingly, each metric will be examined in the context of recent and historical trend information where available. The metric will generally not be considered to constitute a trend until a minimum of statistically significant data points have been established (typically three). Generally, a Status Condition will not be reported as other than "Green" unless a statistically meaningful trend has been established for it.

B.4.2 MDA Core Metrics Report

The MDA Core Metrics are supported by the metrics discussed in the next section. Each Critical Area has complete coverage by the supporting indicator reports. The mapping of supporting metrics to critical areas is shown in the Table below.

Table 4.2-1 Metrics Mapping

Critical Area	Supporting Metrics
Schedule and Progress: this area is concerned with software schedule, task completion, and progress as compared to baselined program plans.	B.4.4.1 Software Schedule Performance B.4.4.2 Software Development Progress B.4.4.3 Sprint Progress B.4.4.4 On-Time Delivery of Software Products B.4.4.5 Software Earned Schedule B.4.4.6 Schedule Performance Index and Schedule Variance B.4.4.7 Functionality and Milestone Progress B.4.4.8 Software Schedule Compression B.4.4.9 Software Unit Testing Progress B.4.4.10 Test and Integration Progress
Cost and Resources: this area ensures adequacy of cost and resources (including personnel) to perform software development work identified in the baselined program plans.	B.4.5.1 Cost Performance Index and Cost Variance B.4.5.2 Supplier Latest Revised Estimate B.4.5.3 Staffing Adequacy B.4.5.4 Software Cost Performance B.4.5.5 Software Staffing B.4.5.6 Software Staffing Profile
Growth and Stability: this area addresses the delivery of the required capability and management of volatility within management-defined ranges.	B.4.6.1 Requirements Volatility Index B.4.6.2 Software Requirements Stability B.4.6.3 Software Size Estimate B.4.6.4 Software Interface Stability B.4.6.5 Software Functionality Stability B.4.6.6 Software Coding Progress
Adequacy, Quality, Safety, and Performance: this area provides evidence of the extent to which safely and securely meets program capability requirements and that the delivered product safely and securely meets the user's intention without failure.	B.4.7.1 Defect Density B.4.7.2 Defect Profile B.4.7.3 Defect Closure B.4.7.4 Defect Containment B.4.7.5 First Time Quality of Software B.4.7.6 Defect History B.4.7.7 Engineering Change Proposal Cycle Time B.4.7.8 Engineering Change Proposal Approval Rate B.4.7.9 Number of Deviation Requests and Percent Recurring B.4.7.10 Change Incorporation Rate B.4.7.11 Completion of Class I Engineering Change Proposals Implementing Actions B.4.7.12 Rework B.4.7.13 Failure Review Board B.4.7.14 Foreign Object Elimination B.4.7.15 Waivers and Deviations B.4.7.16 MRB Actions, Dispositions, and Cost Metrics B.4.7.17 Occupational Safety B.4.7.18 System Safety Progress B.4.7.19 Software Safety Status B.4.7.20 Inherent Availability B.4.7.21 Operational Availability B.4.7.22 Mean Time To Repair B.4.7.23 Mean Time To Restore Functions

	<ul style="list-style-type: none">B.4.7.24 Inherent Mean Time Between Critical FailureB.4.7.25 Operational Mean Time Between Critical FailureB.4.7.26 Mean Logistics Delay TimeB.4.7.27 Mean Repair TimeB.4.7.28 Fault DetectionB.4.7.29 Fault IsolationB.4.7.30 Maintenance Ratio
Software Development Environment: this area addresses the software productivity, languages selected, adoption of software development best practices, exhibited elements of reuse, and efficiency of the software development team.	<ul style="list-style-type: none">B.4.8.1 Software ProductivityB.4.8.2 Software Requirements AmbiguityB.4.8.3 Software Requirements IncompletenessB.4.8.4 Software Reuse ProfileB.4.8.5 Programming Languages ProfileB.4.8.6 Resource UtilizationB.4.8.7 Cyclomatic Complexity

B.4.3 Metrics Indicators

The metrics indicator reports are standardized chart definitions contributing to the completeness of each Critical Area. Each indicator report is made up of data primitives or aggregates of data primitives mapped against another data set (e.g., time, resource, and other primitives).

The indicator reports are expressed in the following format:

- a. **Description:** Description of the metric indicator, the goals of collection, and the questions the metric indicator answers.
- b. **Critical Area:** Describes which Area(s) are addressed by the indicator.
- c. **Application:** Frequency of collection, fidelity of collection, and applicability to programs.
- d. **Data Primitives Collected:** Atomic level data collected.
- e. **Aggregate Values Calculated:** Data collected via formulas of Primitives.
- f. **Scoring Criteria:** Values and levels used in scoring the Indicator Report red, yellow, or green, as appropriate.
- g. **Sample Representation:** Sample graphic displaying how the data might be represented. Where possible, it is preferred to include 6 months of past performance and a 6 month forecast.
- h. **Analysis Methods:** Outlines MDA data analysis goals for each metrics indicator in the areas of Threshold, Parametric, Correlation, and Trend Analysis.
 - 1) **Threshold** - checking program defined error boundaries, subjective review, elimination of delivery/syntactical errors.
 - 2) **Parametric** - use of established tools or models on a subset of primitive data.
 - 3) **Correlation** - comparative analysis between related but distinct software Indicator Reports (i.e. Requirements Volatility vs. Software Size); the correlations listed are suggestions, but in no way limit hypothesized testing of indicator reports.
 - 4) **Trend** - forecasting data points into the future based on confidence intervals, establishing viability of delivery and schedules based on past performance.

Variations or translations for outlying software development lifecycles are detailed in individual reports where applicable.

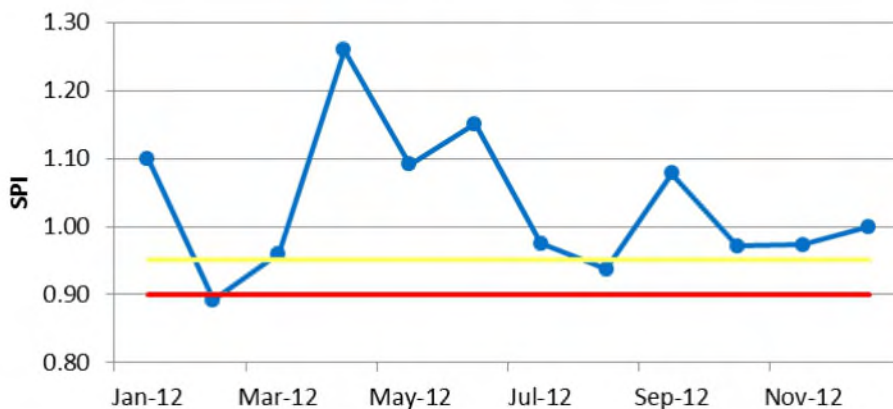
B.4.4 Schedule and Progress

The area of Schedule and Progress addresses the completion of program milestones, significant events, and individual work items. The indicator reports included in Schedule and Progress are:

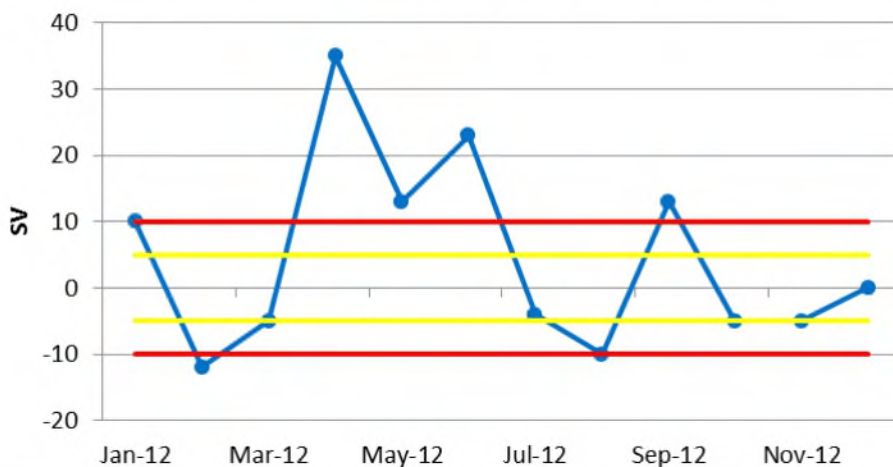
- B.4.4.1 Software Schedule Performance.
- B.4.4.2 Software Development Progress.
- B.4.4.3 Sprint Progress.
- B.4.4.4 On-Time Delivery of Software Products.
- B.4.4.5 Software Earned Schedule.
- B.4.4.6 Schedule Performance Index and Schedule Variance.
- B.4.4.7 Functionality and Milestone Progress.
- B.4.4.8 Software Schedule Compression.
- B.4.4.9 Software Unit Testing Progress.
- B.4.4.10 Test and Integration Progress.

B.4.4.1 Software Schedule Performance

Description	The Software Schedule Performance indicator report is used to assess variations from planned schedule baselines. Indices are measured in terms of Earned Value data for the software specific development efforts. Indications of development inefficiencies are revealed through unfavorable schedule performance variances.
Critical Area	Schedule and Performance
Application	<p>Applicable to all MDA software development programs.</p> <p>Collected monthly, by software build and major component from Requirements Analysis through Sustainment (unless Sustainment is a Level Of Effort activity). Software Schedule should address Earned Value data for software specific tasks.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Are software products being developed in a timely manner according to the baseline schedule? What is the likelihood of software being delivered late?
Data Primitives Collected	<ol style="list-style-type: none"> Budgeted Cost of Work Performed (BCWP) (monthly and cumulative) Budgeted Cost of Work Scheduled (BCWS) (monthly and cumulative).
Aggregate Values Calculated	<ol style="list-style-type: none"> Schedule Performance Index (SPI) = $BCWP/BCWS$ (monthly and cumulative) Schedule Variance (SV) = $BCWP - BCWS$ (monthly and cumulative) $SV\% = (SV / BCWS) \times 100$ (Schedule Variance Percentage)
Scoring Criteria	<p>Scoring Criteria are applied to both current and cumulative to-date values:</p> <p>An SPI value of 1 is nominal and indicates program is on schedule. Values > 1 indicate that the program is ahead of schedule Values < 1 indicate that the program is behind schedule.</p> <p>GREEN: $0.95 \leq SPI \leq 1.05$ YELLOW: $0.90 \leq SPI < 0.95$ or $1.05 < SPI \leq 1.10$ RED: $SPI < 0.90$ or $SPI > 1.10$</p> <p>An SV percentage of 0% is nominal. A positive schedule variance percentage is an indication that in-process work is ahead of schedule. A negative schedule variance percentage indicates that the in-process work is behind schedule.</p> <p>GREEN: $-5\% \leq SV\% \leq 5\%$ YELLOW: $-10\% \leq SV\% < -5\%$ OR $5\% < SV\% \leq 10\%$ RED: $SV\% < -10\%$ OR $SV\% > 10\%$</p>

Sample
RepresentationSoftware Schedule Performance
Index

Software Schedule Variance



	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
BCWP	110	99	120	170	155	175	155	150	180	170	180	190
BCWS	100	111	125	135	142	152	159	160	167	175	185	190
BCWP (cum)	110	99	120	170	155	175	155	150	180	170	180	190
BCWS (cum)	100	111	125	135	142	152	159	160	167	175	185	190
SPI	1.10	0.89	0.96	1.26	1.09	1.15	0.97	0.94	1.08	0.97	0.97	1.00
SPI (cum)	1.10	0.89	0.96	1.26	1.09	1.15	0.97	0.94	1.08	0.97	0.97	1.00
SV	10	-12	-5	35	13	23	-4	-10	13	-5	-5	0
SV (cum)	10	-12	-5	35	13	23	-4	-10	13	-5	-5	0

Analysis
Methods

Threshold: Scoring criteria listed above and subjective review.

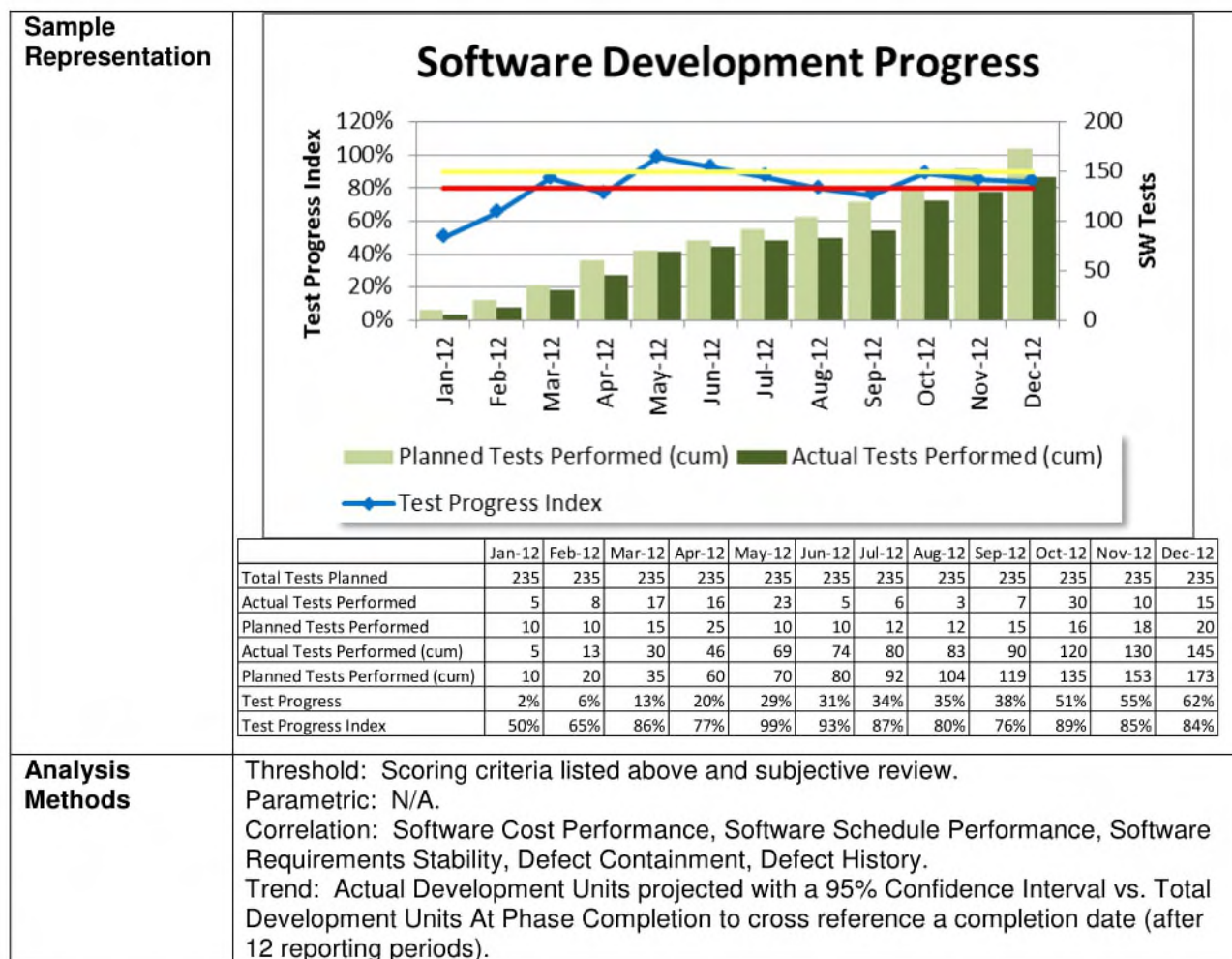
Parametric: Comparison of BCWP and BCWS to existing software schedule model estimates (i.e., commercially available tools as COCOMO II, SEER For Software).

Correlation: Software Cost Performance, Software Development Progress, On-Time Delivery of Software Products, Software Staffing, Software Size, Programming Languages Profile.

Trend: Trend analysis performed on BCWP prior to major program milestones ("Will it arrive on schedule?").

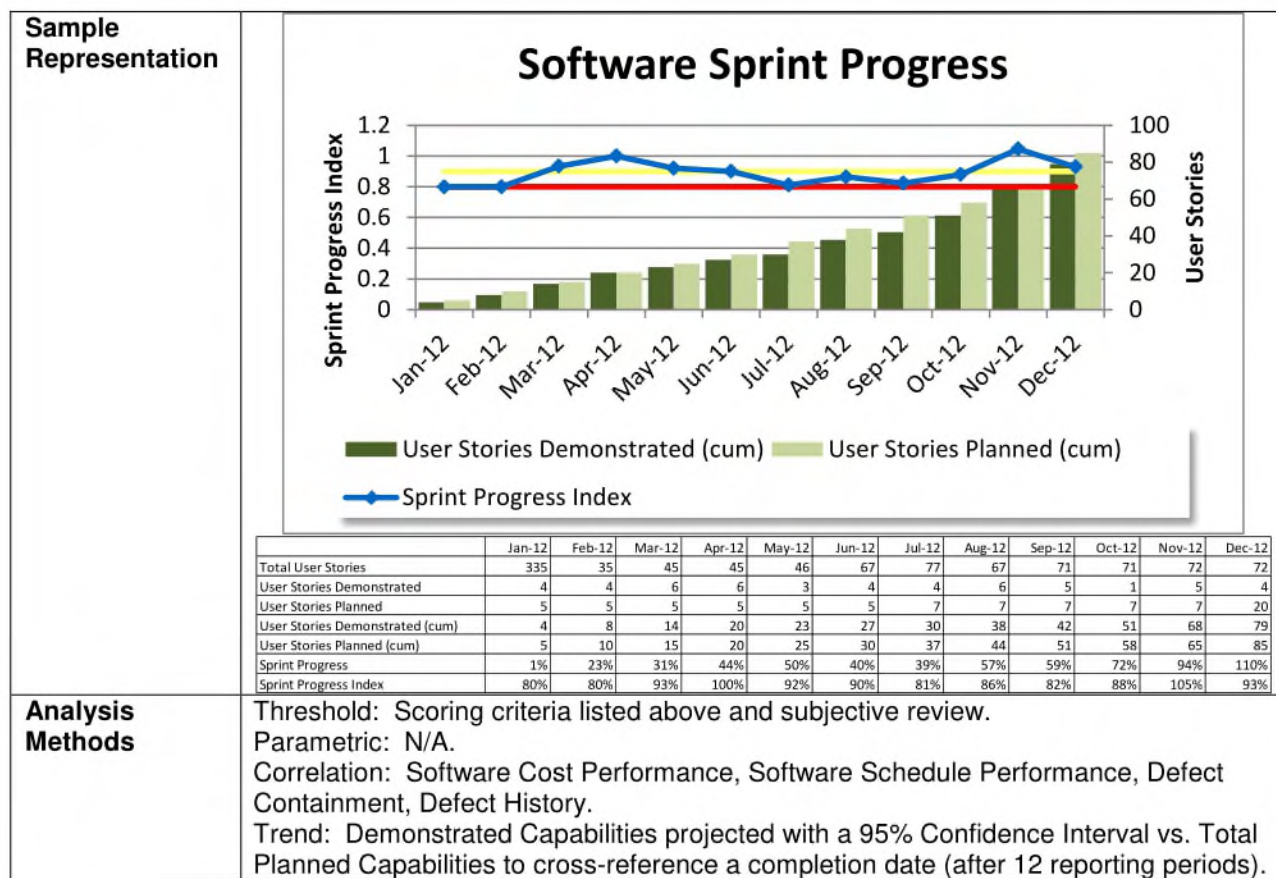
B.4.4.2 Software Development Progress

Description	This metric provides an indication of the software development progress against the planned software development schedule, based on the current life cycle phase. Units are dependent on the current software phase.
Critical Area	Schedule and Performance
Application	<p>Applicable to all MDA software development programs.</p> <p>Collected monthly, by software build and major component from Requirements Analysis through Formal Qualification Testing or equivalent. The units and calculations of development should change and be commiserate with the current development phase. Software Development Progress is collected and captured for every unique software development phase.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Is software development progressing as planned? How much more effort is required in the current software development phase?
Data Primitives Collected	<ol style="list-style-type: none"> Planned Development Units* (monthly and cumulative). Actual Development Units (monthly and cumulative). Total Development Units at Phase Completion. <p><i>* Development Units are defined by the appropriate development phase. Some examples include Requirements Analysis (software requirements specification and Interface Requirement Specification requirements or "shalls"), Design (design walkthroughs, UML objects), Coding (SLOC, Function Points), and Testing (Test Cases).</i></p>
Aggregate Values Calculated	<ol style="list-style-type: none"> Schedule Development Progress Index Percentage = $[\text{Actual Development Units (cumulative)} / \text{Planned Development Units (cumulative)}] \times 100$ Software Development Progress Percentage = $[\text{Actual Development Units (cumulative)} / \text{Total Development Units At Phase Completion}] \times 100$
Scoring Criteria	<p>Software Development Progress Index</p> <p>GREEN: > 90%</p> <p>YELLOW: $90\% \geq \text{Software Development Progress Index} \geq 80\%$</p> <p>RED: < 80%</p>



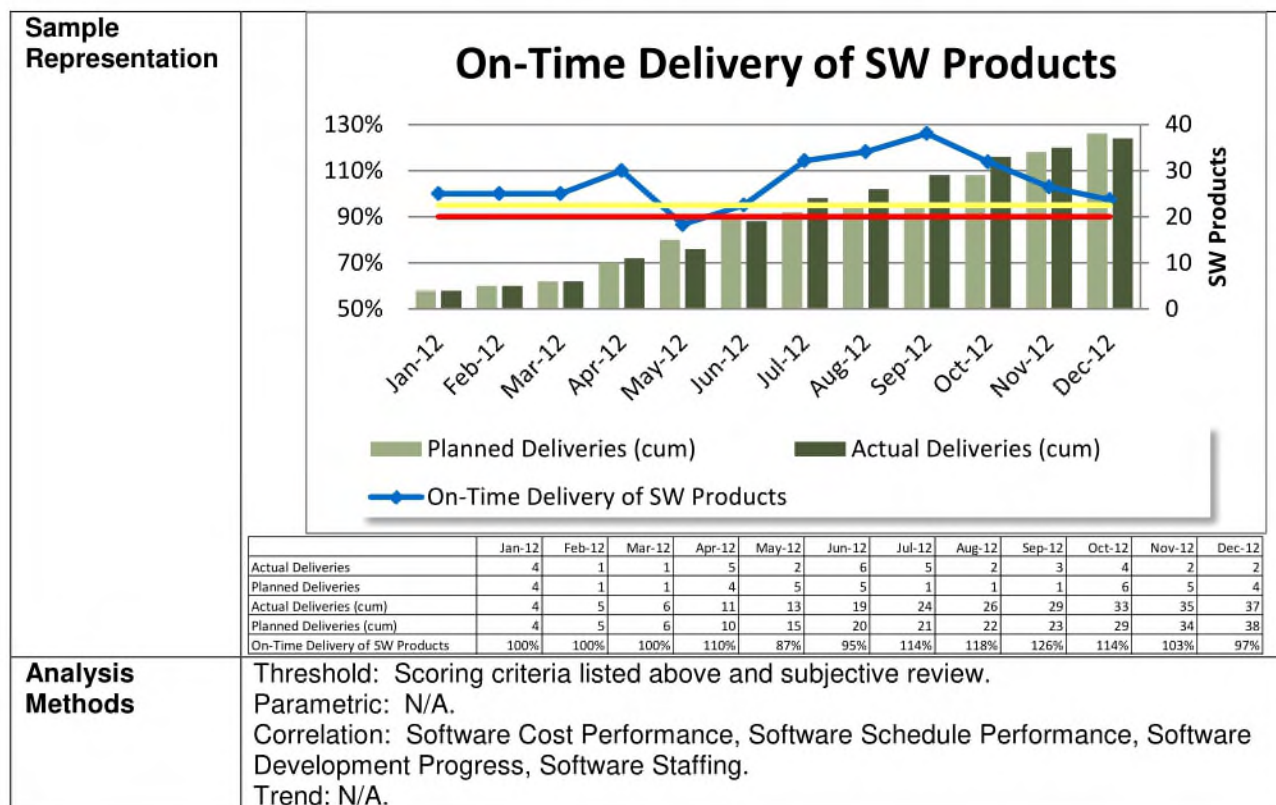
B.4.4.3 Sprint Progress

Description	This metric provides an indication of the software development progress unique to the Agile methodology of Scrum, or any derivation that develops software capabilities in short, concentrated Sprints. It tracks the completion across a planned backlog of demonstrated software capabilities.
Critical Area	Schedule and Performance
Application	<p>Applicable to all MDA software development programs that are using the Agile methodology of Scrum or a derivative that uses Sprints.</p> <p>Collected monthly, by software build and major component across the total project backlog.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Are capabilities being demonstrated in a timely manner? How many more capabilities have yet to be demonstrated?
Data Primitives Collected	<ol style="list-style-type: none"> Planned Capabilities or User Stories (monthly and cumulative). Demonstrated Capabilities or User Stories (monthly and cumulative). Total Planned Capabilities or User Stories (for the entire development)*. <p><i>* It is understood that given the nature of Agile Development that the Total Planned Capability count is subject to much variation and change.</i></p>
Aggregate Values Calculated	<ol style="list-style-type: none"> $\text{Sprint Progress Index Percentage} = \left[\frac{\text{Cumulative Demonstrated Capabilities}}{\text{Cumulative Capabilities}} \right] \times 100$ $\text{Sprint Completion Percentage} = \left[\frac{\text{Cumulative Demonstrated Capabilities}}{\text{Total Planned Capabilities}} \right] \times 100$
Scoring Criteria	<p>Sprint Progress Index</p> <p>GREEN: > 90%</p> <p>YELLOW: 90% ≥ Sprint Progress Index ≥ 80%</p> <p>RED: < 80%</p>



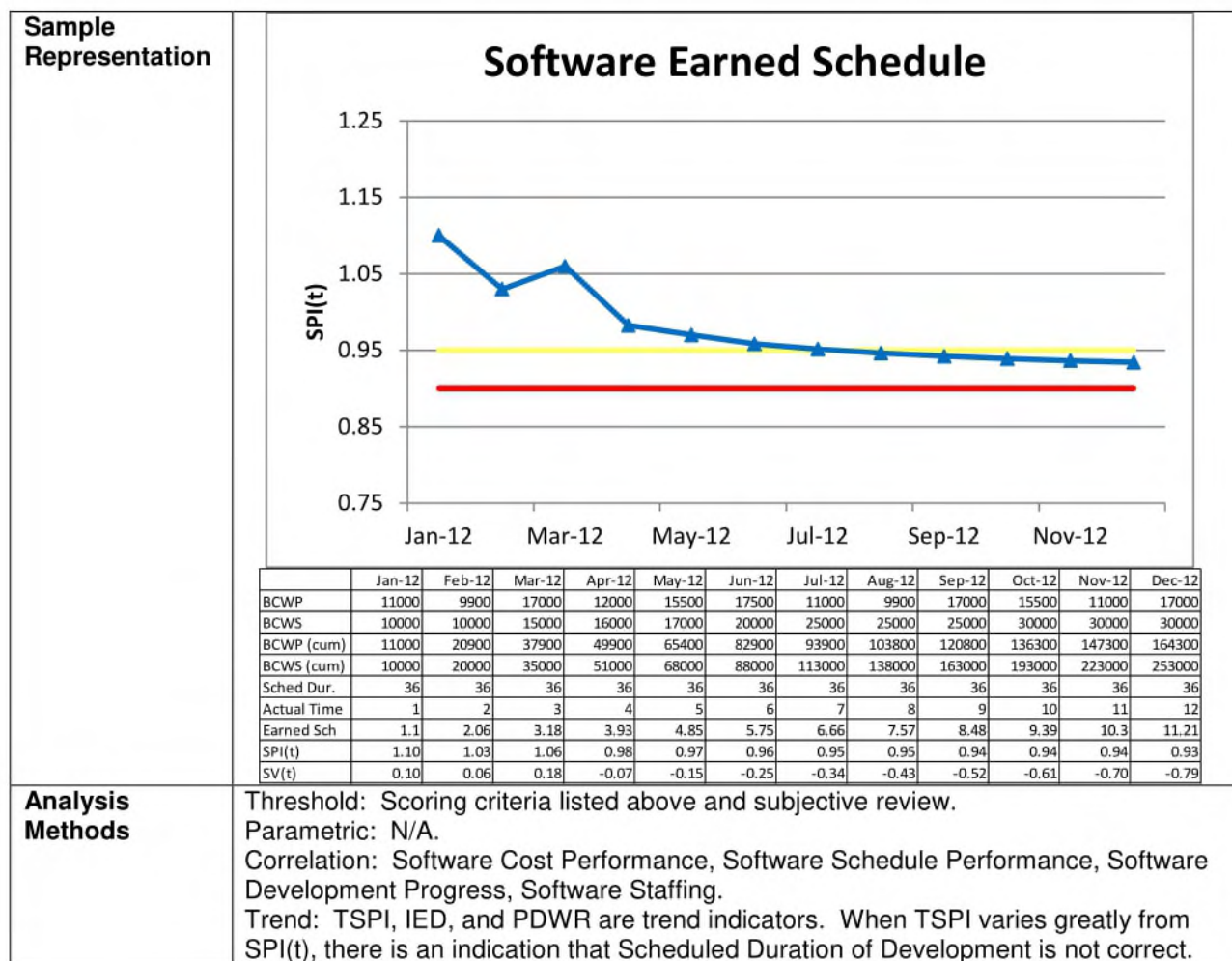
B.4.4.4 On-Time Delivery of Software Products

Description	This metric measures performance to the negotiated/planned delivery schedule for software engineering products. This includes software related CDRL products delivered to an entity beyond the developing organization on a previously agreed upon date.
Critical Area	Schedule and Performance
Application	Applicable to all MDA software development programs. Collected monthly, by software build and major component. Answers the question: Are software products being delivered in a timely manner?
Data Primitives Collected	a. Planned Number of Software Products Scheduled For Delivery (monthly and cumulative). b. Actual Number of Software Products Delivered (monthly and cumulative).
Aggregate Values Calculated	On Time Delivery of Software Products Percentage $= \left[\frac{\text{Actual Number of Software Products Delivered (cumulative)}}{\text{Planned Number of Software Products Scheduled For Delivery (cumulative)}} \right] \times 100$
Scoring Criteria	On-Time Delivery of Software Products GREEN: $\geq 95\%$ YELLOW: $95\% > \text{On-Time Delivery of Software Products} \geq 90\%$ RED: $< 90\%$



B.4.4.5 Software Earned Schedule

Description	This metric provides an indication of the software development progress in terms of calendar time. As opposed to typical Earned Value calculations, Earned Schedule expresses all variances and indices in terms of calendar time, not dollars. Text and tools for Earned Schedule are available at www.earnedschedule.com .
Critical Area	Schedule and Performance
Application	<p>Applicable to all MDA software development programs.</p> <p>Collected monthly, by software build and major component from Requirements Analysis through Sustainment (unless Sustainment is a Level of Effort activity). Software Schedule should address Earned Value data for software specific tasks.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Are software products being developed in a timely manner according to the baseline schedule? How many months is the software development ahead or behind of the baseline schedule?
Data Primitives Collected	<ol style="list-style-type: none"> Budgeted Cost of Work Performed (BCWP) (monthly and cumulative). Budgeted Cost of Work Scheduled (BCWS) (monthly and cumulative). Scheduled Duration of Development (in months). Current Actual Time Elapsed (in months).
Aggregate Values Calculated	<ol style="list-style-type: none"> Target Month = Count of Time In Months where BCWP (cumulative) < BCWS (cumulative, for that month) BCWS (target) = BCWS (cumulative in the Target Month) Earned Schedule = Target Month + ((BCWS(cum) - BCWS(target)) / (BCWS(target+1) - BCWS(target))) Schedule Variance in terms of time (SV(t)) = Current Actual Time Elapsed - Earned Schedule Schedule Performance Index in terms of time (SPI(t)) = Earned Schedule / Current Actual Time Elapsed Independent Estimate of Delivery (IED) = Scheduled Duration of Development / Earned Schedule To-Complete Schedule Performance Index (TSPI) = (Scheduled Duration of Development - Earned Schedule) / (Scheduled Duration of Development - Current Actual Time Elapsed) Predicted Development Work Remaining (PDWR) = Scheduled Duration of Development - Earned Schedule
Scoring Criteria	<p>SPI(t)</p> <p>GREEN: ≥ 0.95.</p> <p>YELLOW: $0.95 > \text{SPI}(t) \geq 0.90$.</p> <p>RED: < 0.90.</p> <p>SV(t)</p> <p>GREEN: > -1.0 months.</p> <p>YELLOW: $-1.0 \text{ months} > \text{SV}(t) \geq -2.0 \text{ months}$.</p> <p>RED: < -2.0 months.</p>

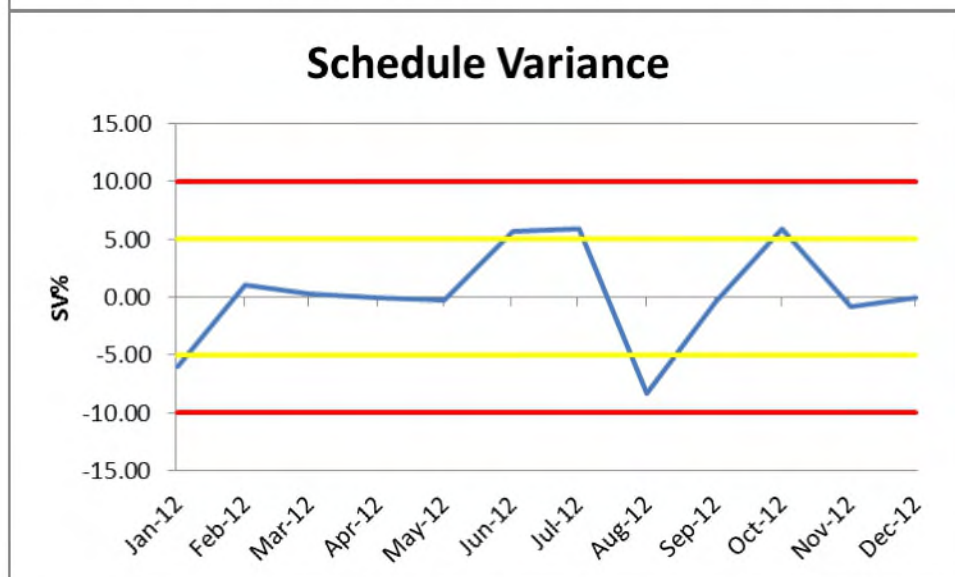
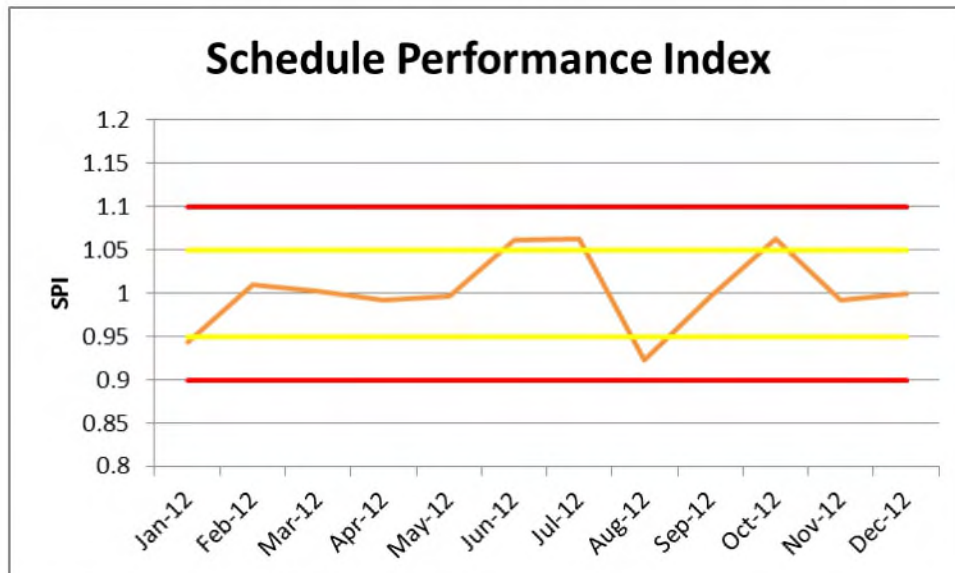


Analysis Methods

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: Software Cost Performance, Software Schedule Performance, Software Development Progress, Software Staffing.
 Trend: TSPI, IED, and PDWR are trend indicators. When TSPI varies greatly from SPI(t), there is an indication that Scheduled Duration of Development is not correct.

B.4.4.6 Schedule Performance Index and Schedule Variance

Description	<p>Schedule Performance Index (SPI) provides a quantitative measure of progress toward meeting the development schedule. Performance indices show percentage of variation, between planned and actual performance, for the current period and cumulative to-date for currently approved WBS and schedule.</p> <p>Schedule Variance (SV) compares budgeted cost of work performed with budgeted cost of work scheduled. A positive schedule variance is an indication that in-process work is ahead of schedule. A negative schedule variance indicates that in-process work is behind schedule.</p>
Critical Area	Schedule and Progress
Application	<p>SPI and SV are applicable to all MDA programs.</p> <p>Answers the question: Are project activities being accomplished in accordance with project schedule?</p>
Data Primitives Collected	<p>Separately report hardware, and software build and major component values* for current and cumulative period. Provide current and cumulative to-date values for:</p> <ol style="list-style-type: none"> Budgeted Cost of Work Performed (BCWP) units (e.g., dollars). Budgeted Cost of Work Scheduled (BCWS). Schedule Performance Index. Schedule Variance. Schedule Variance Percentage (SV%). <p>* Contractor should also provide a description of Earned Value (EV) terms as contractors use different EV tools and this will assist MDA in correctly interpreting EV data.</p>
Aggregate Values Calculated	<p>Calculate current and cumulative to-date values using:</p> <ol style="list-style-type: none"> $SPI = BCWP / BCWS$ $SV = BCWP - BCWS$ $SV\% = (SV / BCWS) \times 100$ (Schedule Variance Percentage)
Scoring Criteria	<p>Scoring Criteria are applied to both current and cumulative to-date values: An SPI value of 1 is nominal and indicates program is on schedule. Values > 1 indicate that the program is ahead of schedule Values < 1 indicate that the program is behind schedule.</p> <p>GREEN: $0.95 \leq SPI \leq 1.05$ YELLOW: $0.90 \leq SPI < 0.95$ or $1.05 < SPI \leq 1.10$ RED: $SPI < 0.90$ or $SPI > 1.10$</p> <p>An SV percentage of 0% is nominal. A positive schedule variance percentage is an indication that in-process work is ahead of schedule. A negative schedule variance percentage indicates that the in-process work is behind schedule.</p> <p>GREEN: $-5\% \leq SV\% \leq 5\%$ YELLOW: $-10\% \leq SV\% < -5\%$ OR $5\% < SV\% \leq 10\%$ RED: $SV\% < -10\%$ OR $SV\% > 10\%$</p>

**Sample
Representation**


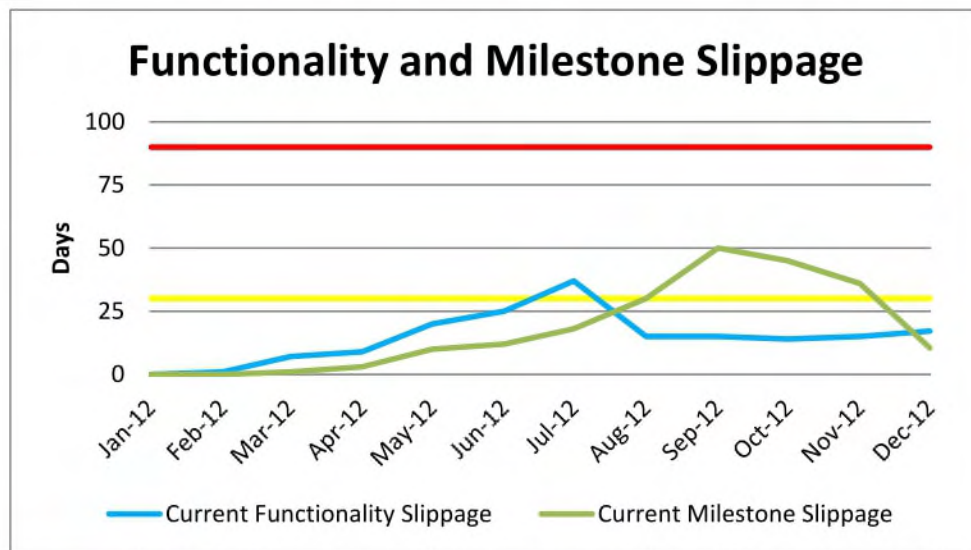
	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
BCWP	11000	9900	17000	12000	15500	17500	17000	12000	15500	17000	12000	15500
BCWS	11658	9800	16958	12090	15547	16500	16000	13000	15559	16000	12099	15499
SPI	0.943558	1.010204	1.002477	0.992556	0.996977	1.060606	1.0625	0.923077	0.996208	1.0625	0.991818	1.000065
SV	-658.00	100.00	42.00	1.01	-47.00	1000.00	1000.00	-1000.00	-59.00	1000.00	-99.00	1.00
SV%	-5.98	1.01	0.25	0.01	-0.30	5.71	5.88	-8.33	-0.38	5.88	-0.83	0.01

**Analysis
Methods**

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

B.4.4.7 Functionality and Milestone Progress

Description	Functionality and Milestone Progress provide a quantitative measure of schedule stability and slippage with regard to functional delivery and program milestone progress.
Critical Area	Schedule and Progress
Application	<p>Functionality and Milestone Progress are applicable to all MDA programs.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> To what extent is progress being made in achieving functional availability? To what extent are milestones being achieved?
Data Primitives Collected	<p>Separately report software build and major component values:</p> <ol style="list-style-type: none"> Original baseline, current baseline, current forecast, and actual functional achievements (i.e., sequence of dates)*. Original baseline, current baseline, current forecast, and actual program milestone achievements (i.e., sequence of dates)*. <p>*Note: Identify basis of any slippage in excess of 10%. In particular, identify when slippage is caused by external event (e.g., organizational redirection or funding cuts).</p>
Aggregate Values Calculated	<p>FUNCTIONALITY PROGRESS</p> <ol style="list-style-type: none"> Current Functionality Slippage: For each planned functionality, compute the difference (in days) between the current baseline date and the current forecast date or date functionality is actually achieved. Baseline Functionality Slippage: For each planned functionality, compute the difference (in days) between the original baseline date and the current forecast date or date functionality is actually achieved. <p>MILESTONE PROGRESS</p> <ol style="list-style-type: none"> Current Milestone Slippage: For each program milestone, compute the difference (in days) between the current baseline date and the current forecast date or date milestone is actually achieved. Baseline Milestone Slippage: For each program milestone, compute the difference (in days) between the original baseline date and the current forecast date or date milestone is actually achieved.
Scoring Criteria	<p>FUNCTIONALITY PROGRESS</p> <p>Current Functionality Slippage:</p> <p>GREEN: < 30 days</p> <p>YELLOW: 30 days ≤ Current Functionality Slippage ≤ 90 days</p> <p>RED: 90 days</p> <p>MILESTONE PROGRESS</p> <p>Current Milestone Slippage:</p> <p>GREEN: < 30 days</p> <p>YELLOW: 30 days ≤ Current Milestone Slippage ≤ 90 days</p> <p>RED: > 90 days</p>

**Sample
Representation**

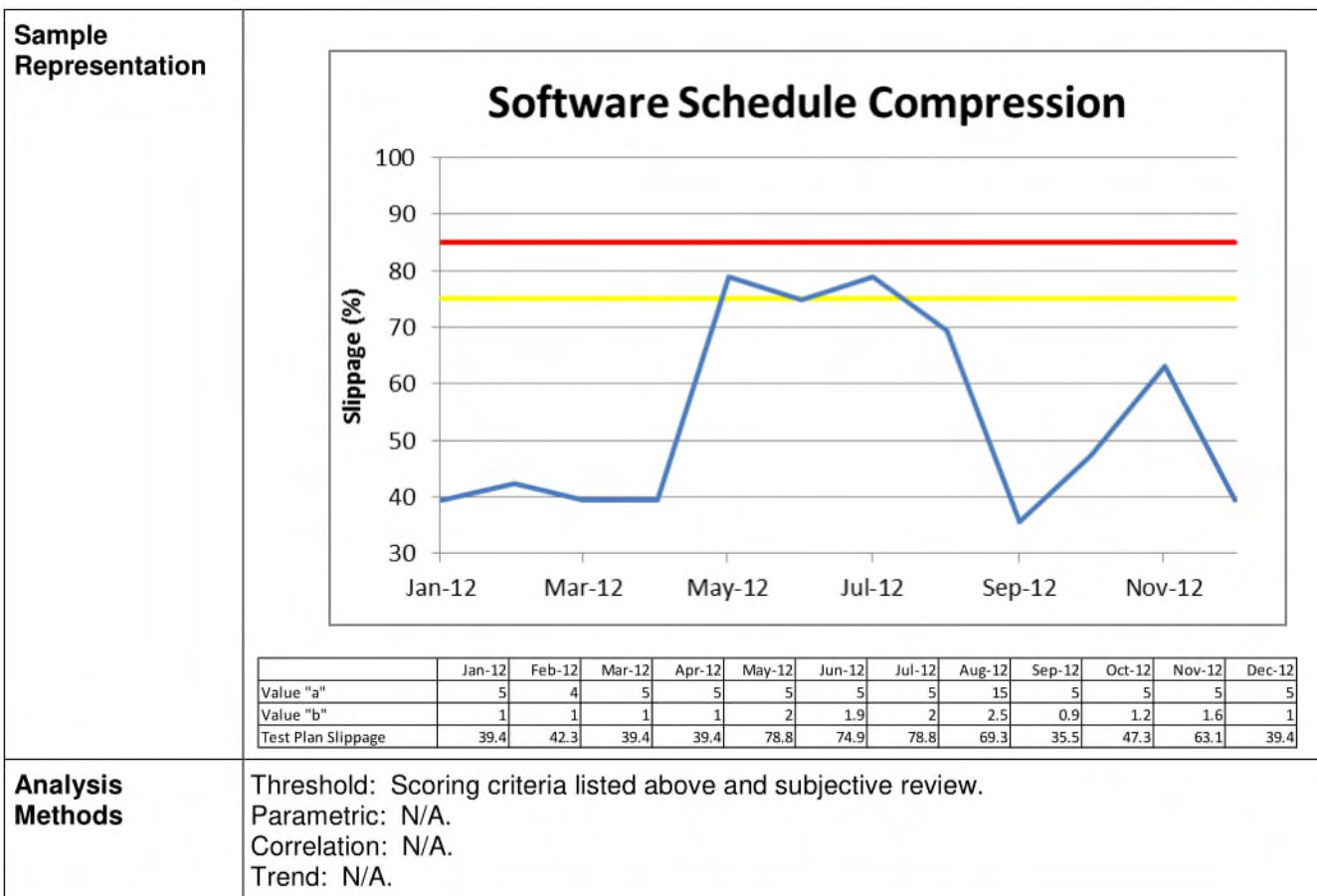
	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Current Functionality Slippage	0	1	7	9	20	25	37	15	15	14	15	17.2
Current Milestone Slippage	0	0	1	3	10	12	18	30	50	45	36	10.5

**Analysis
Methods**

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

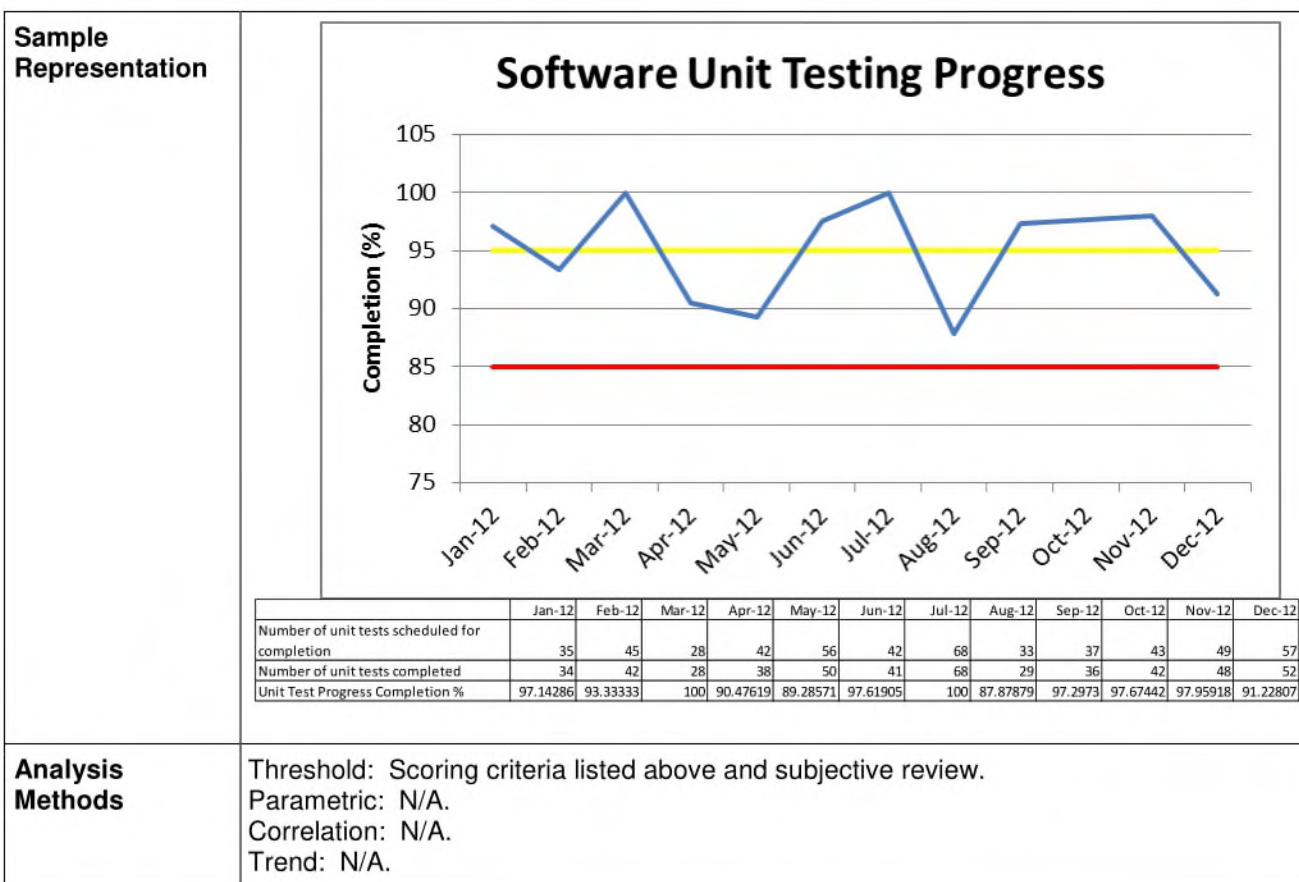
B.4.4.8 Software Schedule Compression

Description	Software Schedule Compression provides a measure of the relationship between planned schedule to complete and nominal schedule* to complete. *See Computational Method below for definition of "nominal schedule."
Critical Area	Schedule and Progress
Application	Software Schedule Compression is applicable to all MDA software development. Answers the questions: a. What is the extent of schedule compression for the remainder of the project's planned efforts? b. How realistic is the planned schedule to complete the remaining project effort?
Data Primitives Collected	Report software build and major component current values: a. Estimated Remaining Effort (estimated staff months of effort for all remaining tasks through software integration and test). b. Estimated Remaining Schedule (estimated schedule months to complete all remaining tasks through software integration and test).
Aggregate Values Calculated	Calculate software build and major component current values: a. Remaining Nominal Schedule Months = $3.67 \times (\text{Value "a"})^{0.32}$ (The values used in this formula are industry standard, refer to the University of Southern California's Center for Software Engineering COCOMO II model used in software cost estimation) b. Remaining Schedule Compression Percentage = $((\text{Value "b"}) / (3.67 \times (\text{Value "a"})^{0.32})) \times 100$
Scoring Criteria	Remaining Schedule Compression: GREEN: > 85% YELLOW: $75\% \leq \text{Remaining Schedule Compression} \leq 85\%$ RED: < 75%



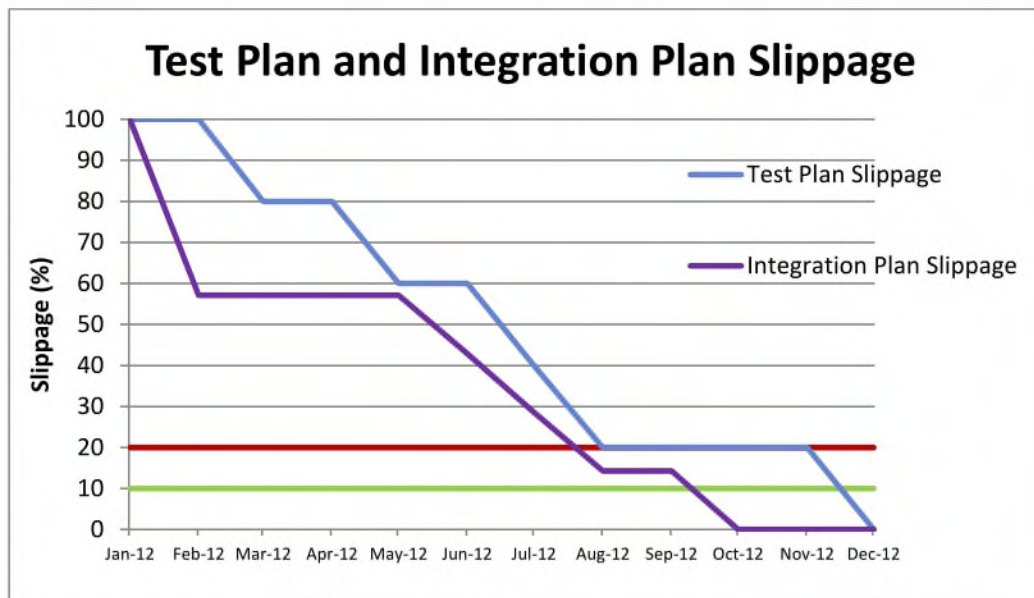
B.4.4.9 Software Unit Testing Progress

Description	Software Unit Testing Progress provides a measure of progress against scheduled unit testing.
Critical Area	Schedule and Progress
Application	Software Unit Testing Progress is applicable to all MDA software development programs. Answers the question: What is the progress of actual unit testing against the planned unit test schedule?
Data Primitives Collected	Separately report BMD Element software component monthly and cumulative: a. Number of unit tests scheduled for completion. b. Number of unit tests completed. Note: Completion is defined as successfully passing unit testing and peer review.
Aggregate Values Calculated	$\text{Unit Test Progress Completion Percentage} = \left[\frac{\text{Value } b}{\text{Value } a} \right] \times 100$
Scoring Criteria	Unit Test Progress Completion % GREEN: > 95% YELLOW: 85% ≤ Unit Progress Completion % ≤ 95% RED: < 85%



B.4.4.10 Test and Integration Progress

Description	Test and Integration Progress provides a quantitative measure of execution against planned test and integration events.
Critical Area	Schedule and Progress
Application	<p>Test and Integration Progress is applicable to all MDA programs.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> To what extent are test events being met on schedule? To what extent are integration events being met on schedule?
Data Primitives Collected	<p>Separately report hardware, and software build and major component values for current and cumulative period:</p> <ol style="list-style-type: none"> Number of originally planned test events. Number of these test events executed. Number of these test events completed. Number of these test events successfully passed. Number of originally planned integration events. Number of these integration events attempted. Number of these integration events completed.
Aggregate Values Calculated	<p>Separately report hardware, and software build and major component computational values for current and cumulative period:</p> <ol style="list-style-type: none"> $\text{Test Plan Slippage Percentage} = \left[\frac{\text{Value a} - \text{Value d}}{\text{Value a}} \right] \times 100$ $\text{Integration Plan Slippage Percentage} = \left[\frac{\text{Value e} - \text{Value g}}{\text{Value e}} \right] \times 100$
Scoring Criteria	<p>Test Plan Slippage</p> <p>GREEN: < 10%</p> <p>YELLOW: $10\% \leq \text{Test Plan Slippage} \leq 20\%$</p> <p>RED: > 20%</p> <p>Integration Plan Slippage</p> <p>GREEN: < 10%</p> <p>YELLOW: $10\% \leq \text{Integration Plan Slippage} \leq 20\%$</p> <p>RED: > 20%</p>

**Sample
Representation**

	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Value "a"	5	5	5	5	5	5	5	5	5	5	5	5
Value "d"	0	0	1	1	2	2	3	4	4	4	4	5
Value "e"	7	7	7	7	7	7	7	7	7	7	7	7
Value "g"	0	3	3	3	3	4	5	6	6	7	7	7
Test Plan Slippage	100.0	100.0	80.0	80.0	60.0	60.0	40.0	20.0	20.0	20.0	20.0	0.0
Integration Plan Slippage	100.0	57.1	57.1	57.1	57.1	42.9	28.6	14.3	14.3	0.0	0.0	0.0

**Analysis
Methods**

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

B.4.5 Cost and Resources

Cost and Resources metrics provide insight of contractor's planned and actual costs, and staffing. The indicator reports included in Cost and Resources are:

B.4.5.1 Cost Performance Index and Cost Variance.

B.4.5.2 Supplier Latest Revised Estimate.

B.4.5.3 Staffing Adequacy.

B.4.5.4 Software Cost Performance.

B.4.5.5 Software Staffing.

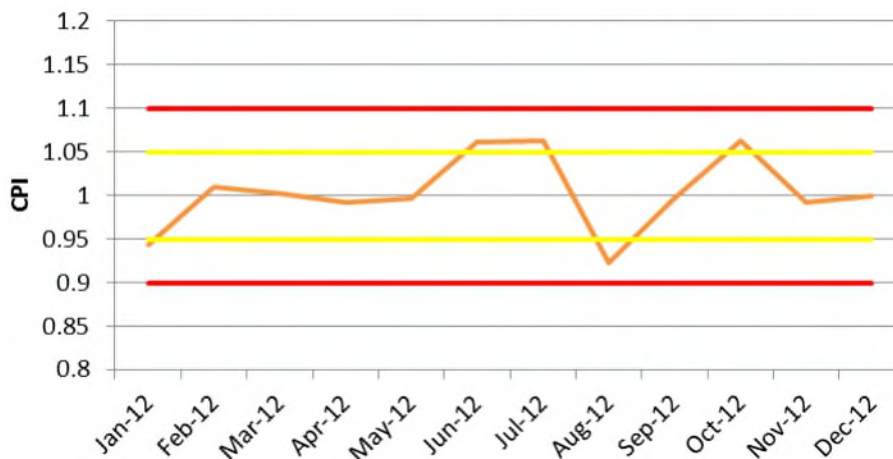
B.4.5.6 Software Staffing Profile.

B.4.5.1 Cost Performance Index and Cost Variance

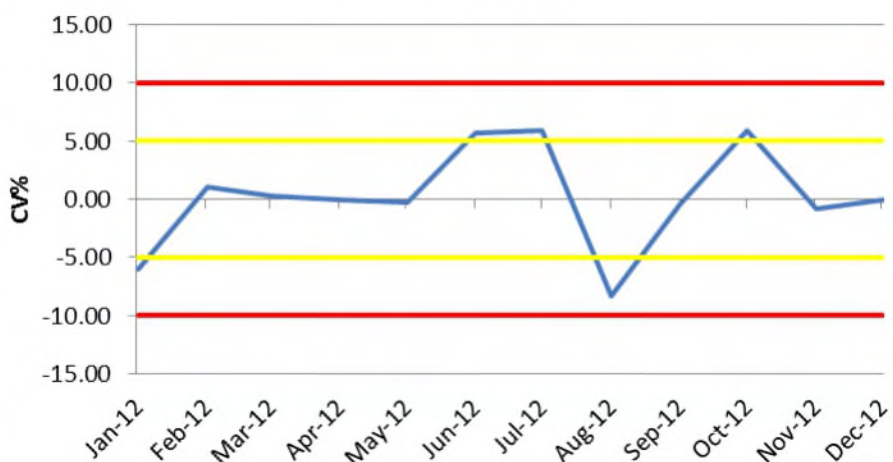
Description	<p>Cost Performance Index (CPI) is an earned value performance factor representing cost efficiency. Cost Performance Index is defined as the ratio of Budgeted Cost of Work Performed (BCWP) versus Actual Cost of Work Performed (ACWP).</p> <p>Cost Variance (CV) is the difference between actual and budgeted cost of work performed. Any departure from the budgeted spending profile will appear as a variance.</p>
Critical Area	Cost and Resources
Application	<p>The CPI and CV are applicable to all MDA programs.</p> <p>Answers the question:</p> <p>Is the project accomplishing planned work within planned budget?</p>
Data Primitives Collected	<p>Separately report hardware, and software build and major component or CSI values* for current and cumulative period.</p> <ol style="list-style-type: none"> Budgeted Cost of Work Performed. Actual Cost of Work Performed. Cost Performance Index. Cost Variance. Cost Variance Percentage. Percent Level Of Effort (LOE)**. <p>* Contractors should also provide an identification of these and other Earned Value (EV) units as used within their accounting system.</p> <p>** Each component of LOE is to be separately identified and described.</p>
Aggregate Values Calculated	<p>Calculate hardware, and software build and major component or CSI values for current and cumulative period using the following equations:</p> <ol style="list-style-type: none"> $CPI = BCWP / ACWP$ $CV = BCWP - ACWP$ $CV\% = (CV / BCWP) \times 100$ (Cost Variance Percentage) $LOE\% = (ACWP \text{ LOE (for LOE tasks)} / ACWP \text{ TOTAL (total for all tasks)}) \times 100$
Scoring Criteria	<p>A CPI value of 1 is nominal. Values > 1 indicate that the program is under budget. Values < 1 indicate cost overruns.</p> <p>GREEN: $0.95 \leq CPI \leq 1.05$ YELLOW: $0.90 \leq CPI < 0.95$ or $1.05 < CPI \leq 1.10$ RED: $CPI < 0.90$ or $CPI > 1.10$</p> <p>A CV percentage value of 0 is nominal. A positive CV percentage indicates that work was accomplished for less resource expenditure than planned. A negative CV percentage indicates that work accomplished cost more than planned resource value.</p> <p>GREEN: $-5\% \leq CV\% \leq 5\%$ YELLOW: $-10\% \leq CV\% < -5\%$ OR $5\% < CV\% \leq 10\%$ RED: $CV\% < -10\%$ OR $CV\% > 10\%$</p>

Sample
Representation

Cost Performance Index



Cost Variance



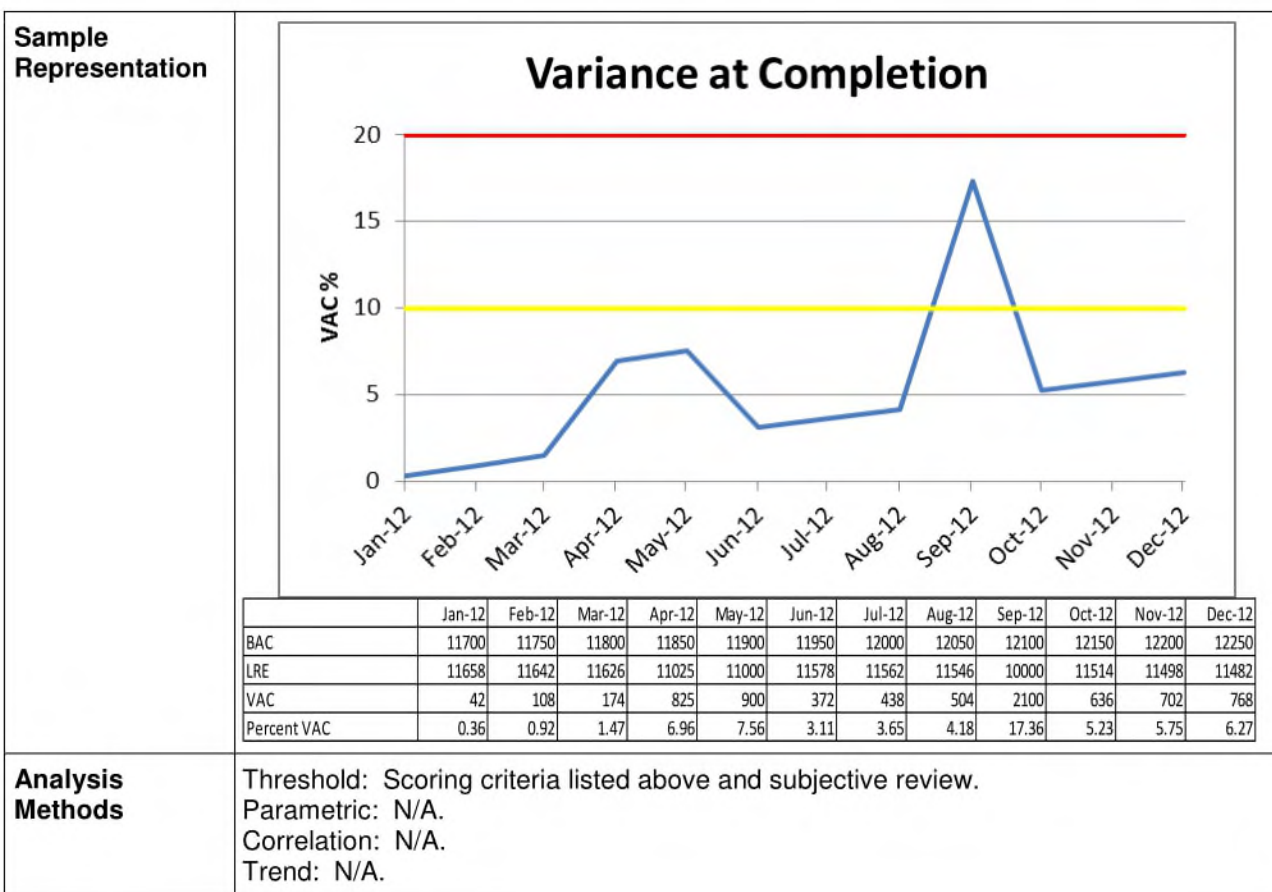
	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
BCWP	11000	9900	17000	12000	15500	17500	17000	12000	15500	17000	12000	15500
ACWP	11658	9800	16958	12090	15547	16500	16000	13000	15559	16000	12099	15499
CPI	0.943558	1.010204	1.002477	0.992556	0.996977	1.060606	1.0625	0.923077	0.996208	1.0625	0.991818	1.000065
CV	-658.00	100.00	42.00	1.01	-47.00	1000.00	1000.00	-1000.00	-59.00	1000.00	-99.00	1.00
CV%	-5.98	1.01	0.25	0.01	-0.30	5.71	5.88	-8.33	-0.38	5.88	-0.83	0.01

Analysis
Methods

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

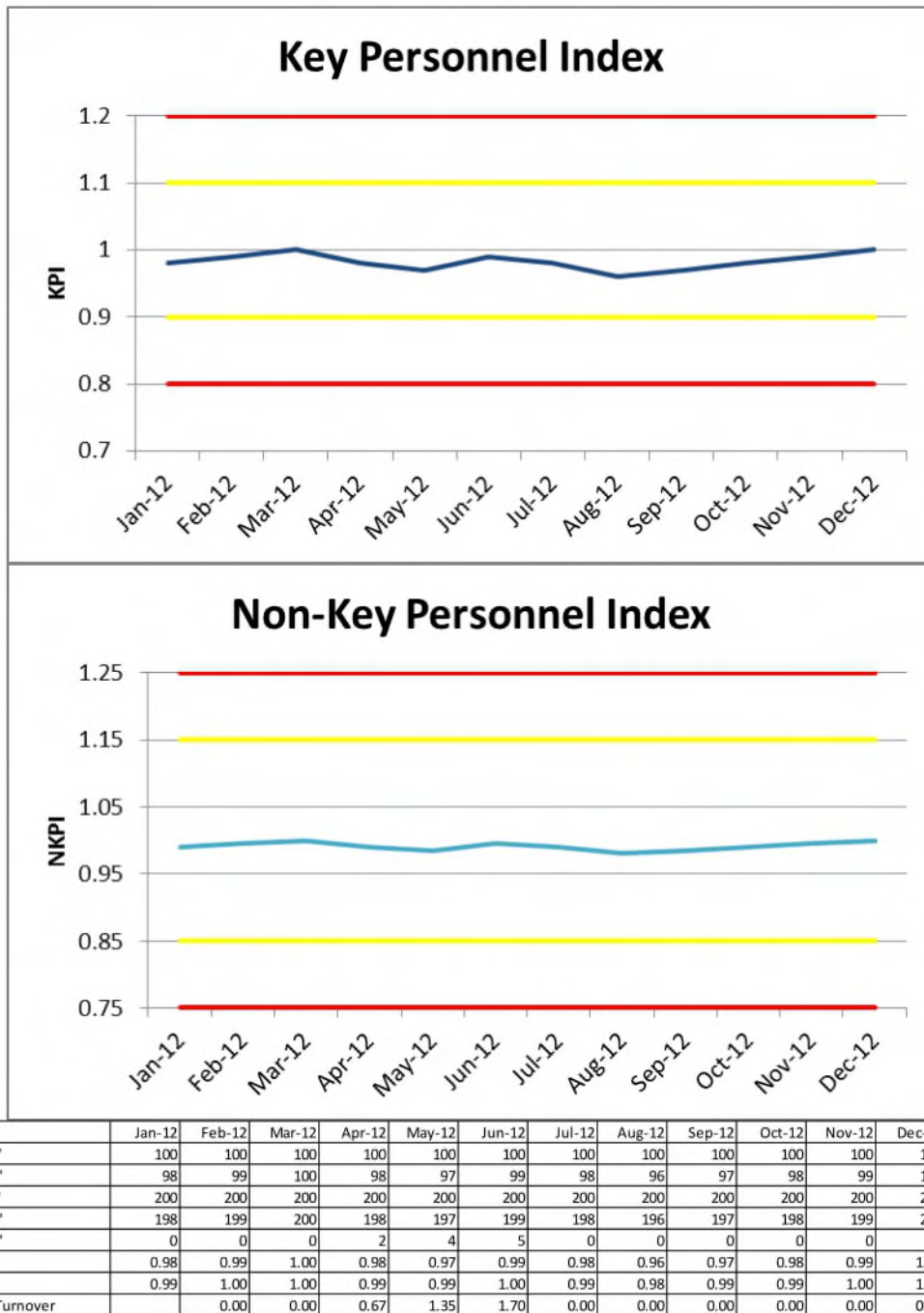
B.4.5.2 Supplier Latest Revised Estimate

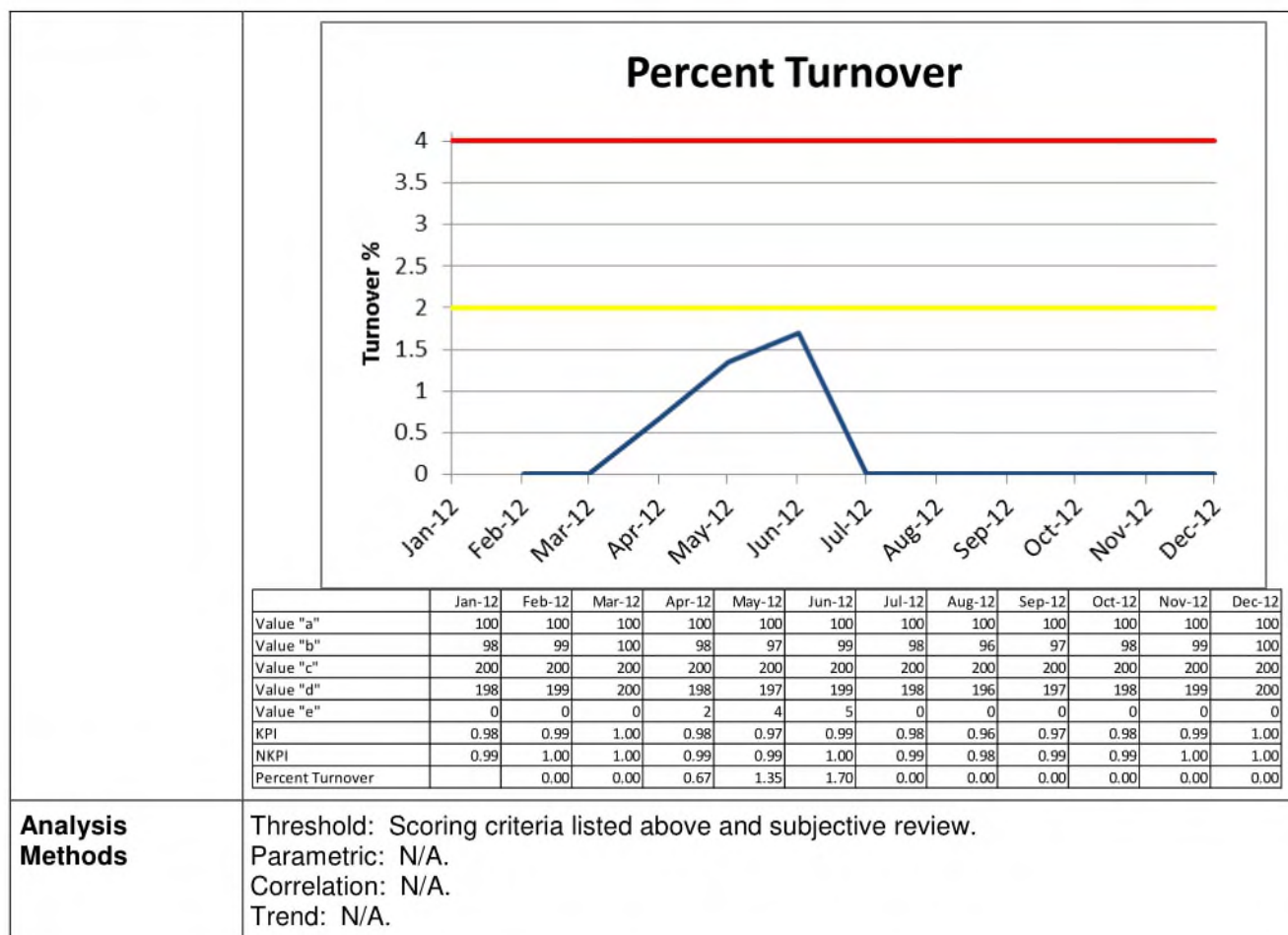
Description	Supplier Latest Revised Estimate (LRE) provides a quantitative measure of anticipated cost of contract at completion, assuming completion of all planned tasks.
Critical Area	Cost and Resources
Application	Supplier LRE is applicable to all MDA programs. Answers the questions: a. How does estimated total cost at contract completion compare with budgeted total cost at completion? b. Will the contract development effort be completed within budgeted cost?
Data Primitives Collected	Separately report hardware, and software build and major component values: a. Supplier LRE* b. Budget at Completion (BAC) * Provide description of analytical method and formulas utilized in determining LRE.
Aggregate Values Calculated	Calculate hardware, and software build and major component values using the following equations: a. Variance at Completion (VAC) = BAC - LRE b. Percent VAC = $[VAC / BAC] \times 100$
Scoring Criteria	Percent VAC: GREEN: < 10% YELLOW: $10\% \leq \text{Percent VAC} \leq 20\%$ RED: > 20%



B.4.5.3 Staffing Adequacy

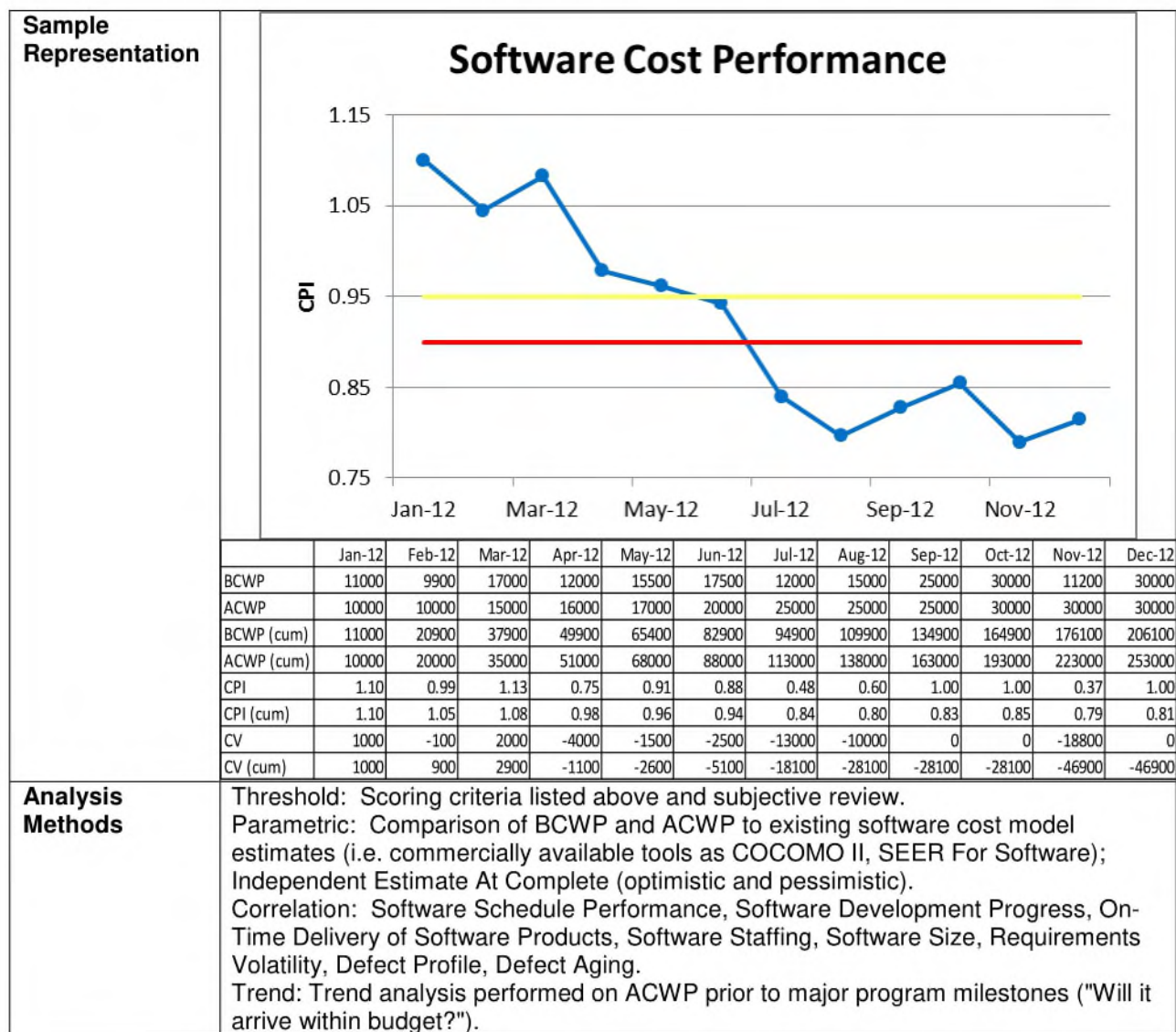
Description	Staffing Adequacy provides a measure of the extent to which staffing is in accordance with the staffing plan.
Critical Area	Cost and Resources
Application	<p>This metric is applicable to all MDA efforts at the software, hardware, and system levels.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Is the organization meeting staffing plans? Is staffing turnover an issue on the program?
Data Primitives Collected	<p>Separately report software, hardware, and system component values for the current period.</p> <ol style="list-style-type: none"> Planned number of key personnel* required on program. Actual number of key personnel* working on program. Planned number of non-key personnel required on program. Actual number of non-key personnel working on program. Actual number of unplanned losses of personnel. <p>*Key personnel are those individuals as defined in the contract who are critical for successful program execution.</p>
Aggregate Values Calculated	<ol style="list-style-type: none"> Key Personnel Index (KPI) = Value "b" / Value "a" Non-Key Personnel Index (NKPI) = Value "d" / Value "c" Percent Turnover = Value "e" / (Value "b" [previous reporting period] + Value "d" [previous reporting period]) × 100
Scoring Criteria	<p>GREEN: $0.90 < KPI < 1.10$, and $0.85 < NKPI < 1.15$, and Percent Turnover < 2%</p> <p>YELLOW: $0.80 \leq KPI \leq 0.90$ OR $1.10 \leq KPI \leq 1.20$, and $0.75 \leq NKPI \leq 0.85$ OR $1.15 \leq NKPI \leq 1.25$, and $2\% \leq \text{Percent Turnover} \leq 4\%$</p> <p>RED: $KPI < 0.80$ OR $KPI > 1.20$ $NKPI < 0.75$ OR $NKPI > 1.25$ Percent Turnover > 4%</p>

Sample
Representation



B.4.5.4 Software Cost Performance

Description	The Software Cost Performance indicator report is used to assess variations from planned cost baselines. Indices are measured in terms of cumulative costs for software development efforts for each software specific effort. The adequacy of a budget to pay for the intended development is examined each month through analysis of the Software Cost Performance indicator. Indications of development inefficiencies are revealed through unfavorable cost performance metrics.
Critical Area	Cost and Resources
Application	<p>Applicable to all MDA software development programs</p> <p>Collected monthly, by software build and major component from Requirements Analysis through Sustainment. Software Cost Performance should address Earned Value data for software specific tasks.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Are software products being developed within budget according to the baselined plan? What is the likelihood that software developments will be delivered for the budgeted cost?
Data Primitives Collected	<ol style="list-style-type: none"> Budgeted Cost of Work Performed (BCWP) (monthly and cumulative). Actual Cost of Work Performed (ACWP) (monthly and cumulative). Budget At Completion (BAC). Estimate At Completion (EAC).
Aggregate Values Calculated	<ol style="list-style-type: none"> Cost Performance Index (CPI) = $BCWP/ACWP$ (monthly and cumulative) Cost Variance (CV) = $BCWP - ACWP$ (monthly and cumulative) Variance At Completion (VAC) = $BAC - EAC$ To Complete Performance Index (TCPI) = $(BAC - BCWP)/(EAC - ACWP)$ Percent Complete = $BCWP/BAC \times 100$
Scoring Criteria	<p>CPI (cumulative)</p> <p>GREEN: ≥ 0.95</p> <p>YELLOW: $0.95 > CPI \text{ (cumulative)} \geq 0.90$</p> <p>RED: < 0.90</p> <p>TCPI (when Percent Complete >20%)</p> <p>GREEN: $TCPI - CPI \leq 0.05$</p> <p>YELLOW: $0.05 < TCPI - CPI \leq 0.15$</p> <p>RED: $TCPI - CPI > 0.15$</p>



Analysis Methods

Threshold: Scoring criteria listed above and subjective review.

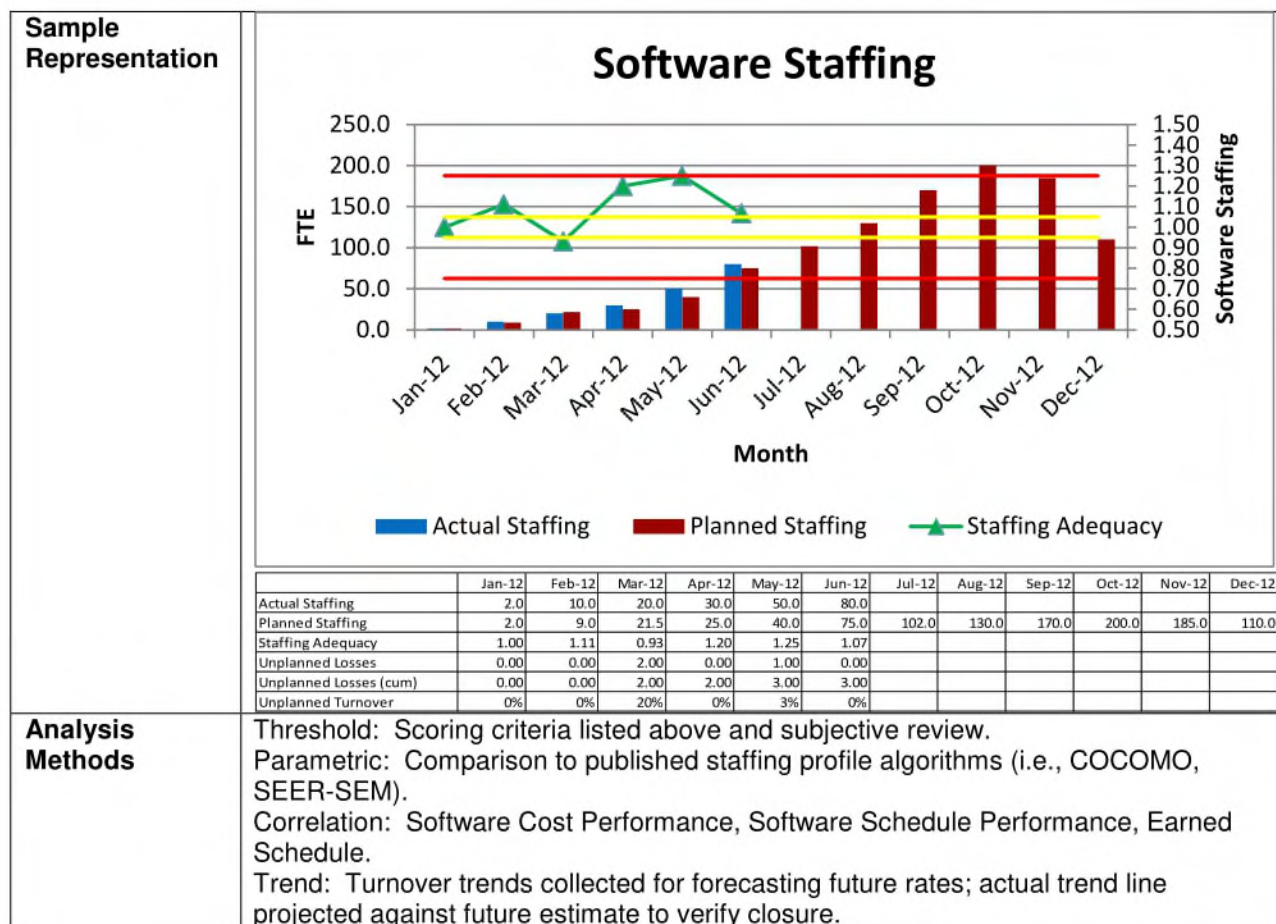
Parametric: Comparison of BCWP and ACWP to existing software cost model estimates (i.e. commercially available tools as COCOMO II, SEER For Software); Independent Estimate At Complete (optimistic and pessimistic).

Correlation: Software Schedule Performance, Software Development Progress, On-Time Delivery of Software Products, Software Staffing, Software Size, Requirements Volatility, Defect Profile, Defect Aging.

Trend: Trend analysis performed on ACWP prior to major program milestones ("Will it arrive within budget?").

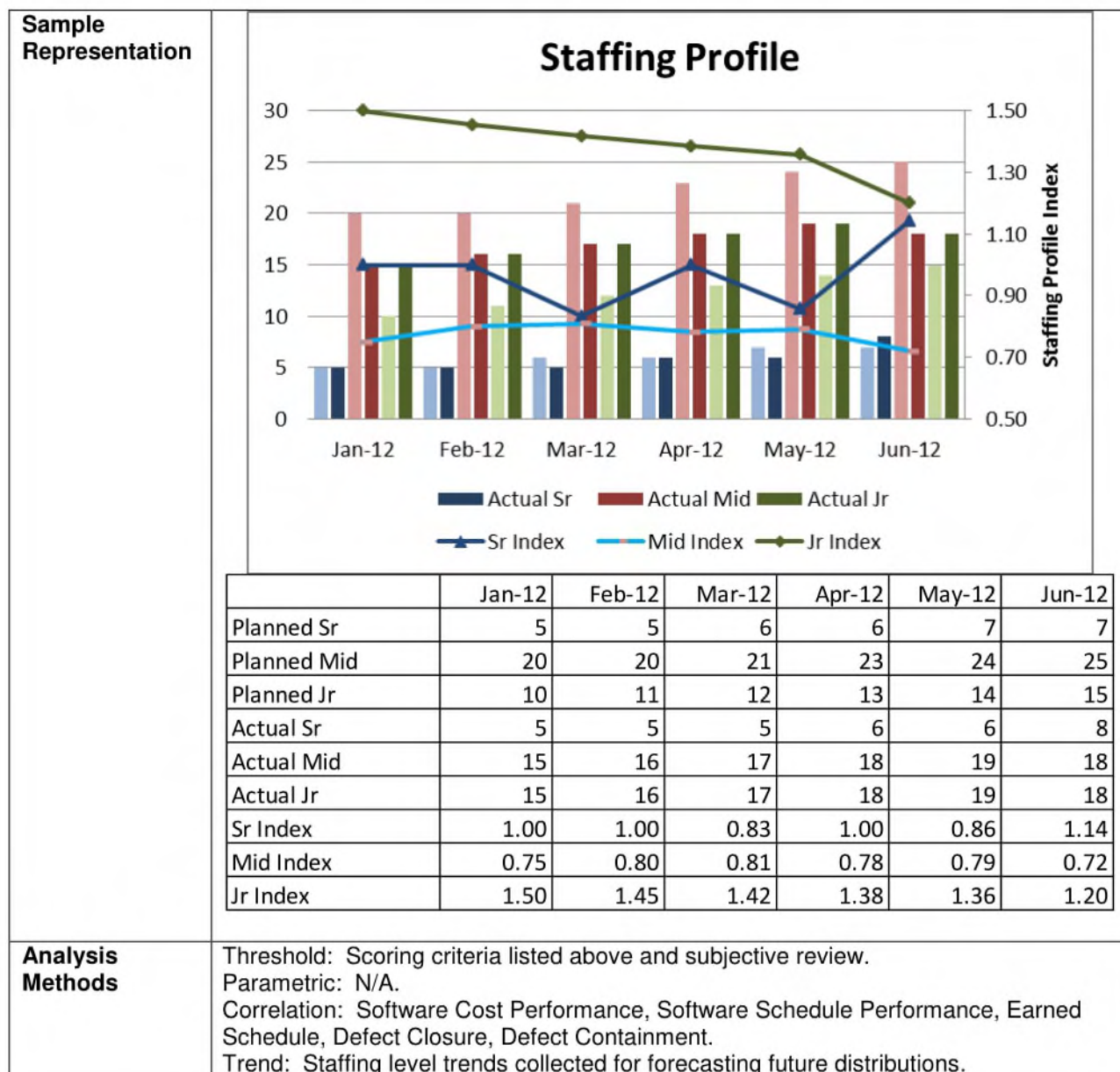
B.4.5.5 Software Staffing

Description	<p>The Software Staffing indicator report tracks planned and actual levels of software development personnel. Planned additions to staff are tracked. Unexpected losses (i.e., resignations, transfers, and terminations not due to planned program changes) are also tracked on a monthly basis. The numbers are expressed in equivalent personnel (EP), where two individuals each working half-time are recorded as 1.0 EP, as opposed to counting "heads."</p> <p>"Staff" consists of all personnel directly contributing to the software activities. Examples would include such job titles as: Programmer, Senior Programmer, Analyst, Supervisor, Technical Writer, Department Head, Tester, and Reviewer.</p>
Critical Area	Cost and Resources
Application	<p>Applicable to all MDA software development programs</p> <p>Collected monthly, by software build and major component from Requirements Analysis through Sustainment.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Is the software program properly staffed for the baselined effort? Is unplanned turnover a source of risk for the software program?
Data Primitives Collected	<ol style="list-style-type: none"> Planned Staff Level (monthly). Actual Staff Level (monthly). Unplanned Losses (monthly and cumulative).
Aggregate Values Calculated	<ol style="list-style-type: none"> Software Staffing = Actual Staff Level / Planned Staff Level Unplanned Turnover Percentage = Unplanned Losses (current month) / Actual Staff Level (from previous month) × 100
Scoring Criteria	<p>Software Staffing</p> <p>GREEN: $1.05 \geq \text{Software Staffing} \geq 0.95$</p> <p>YELLOW: $1.25 \geq \text{Software Staffing} > 1.05$ OR $0.75 \leq \text{Software Staffing} < 0.95$</p> <p>RED: $\text{Software Staffing} > 1.25$ OR $\text{Software Staffing} < 0.75$</p> <p>Unplanned Turnover</p> <p>GREEN: $\leq 2\%$</p> <p>YELLOW: $2\% < \text{Unplanned Turnover} \leq 5\%$</p> <p>RED: $\text{Unplanned Turnover} > 5\%$</p>



B.4.5.6 Software Staffing Profile

Description	<p>The Software Staffing Profile indicator report tracks planned and actual levels of software development personnel in terms of levels of experience. Overages in junior level software personnel results in a quality risk for the product. Overages in senior level software personnel results in a cost risk for the product. Overage or underage in mid-level staff could indicate staffing estimation risk hidden by labor mix variation. The numbers are expressed in equivalent personnel (EP), where two individuals each working half-time are recorded as 1.0 EP, as opposed to counting "heads."</p> <p>Here, a Senior Level Software Staff employee has 10 or more years of salient software experience. A Mid-Level Software Staff employee has 5 or more years salient software experience. Junior Software Staff employees have less than 5 years of salient software experience.</p>
Critical Area	Cost and Resources
Application	<p>Applicable to all MDA software development programs</p> <p>Collected monthly, by software build and major component from Requirements Analysis through Sustainment.</p> <p>Answers the question:</p> <p>Does the software program have a sufficient labor mix to address the baselined effort?</p>
Data Primitives Collected	<ul style="list-style-type: none"> a. Planned Number of Senior Staff (monthly) b. Planned Number of Mid-Level Staff (monthly) c. Planned Number of Junior Staff (monthly) d. Actual Number of Senior Staff (monthly) e. Actual Number of Mid-Level Staff (monthly) f. Actual Number of Junior Staff (monthly)
Aggregate Values Calculated	<ul style="list-style-type: none"> a. Senior Staff Index = Actual Senior Staff / Planned Senior Staff b. Mid-Level Staff Index = Actual Mid-Level Staff / Planned Mid-Level Staff c. Junior Staff Index = Actual Junior Staff / Planned Junior Staff
Scoring Criteria	<p>Any Level Staff Index</p> <p>GREEN: $1.10 \geq \text{Staff Index} \geq 0.90$</p> <p>YELLOW: $1.10 < \text{Staff Index} \leq 1.25$ OR $0.90 > \text{Staff Index} \geq 0.75$</p> <p>RED: $\text{Staff Index} > 1.25$ OR $\text{Staff Index} < 0.75$</p>



B.4.6 Growth and Stability

The area of Growth and Stability addresses the delivery of the required capability and management of volatility within management-defined ranges. The growth and Stability indicators are:

B.4.6.1 Requirements Volatility Index.

B.4.6.2 Software Requirements Stability.

B.4.6.3 Software Size Estimate.

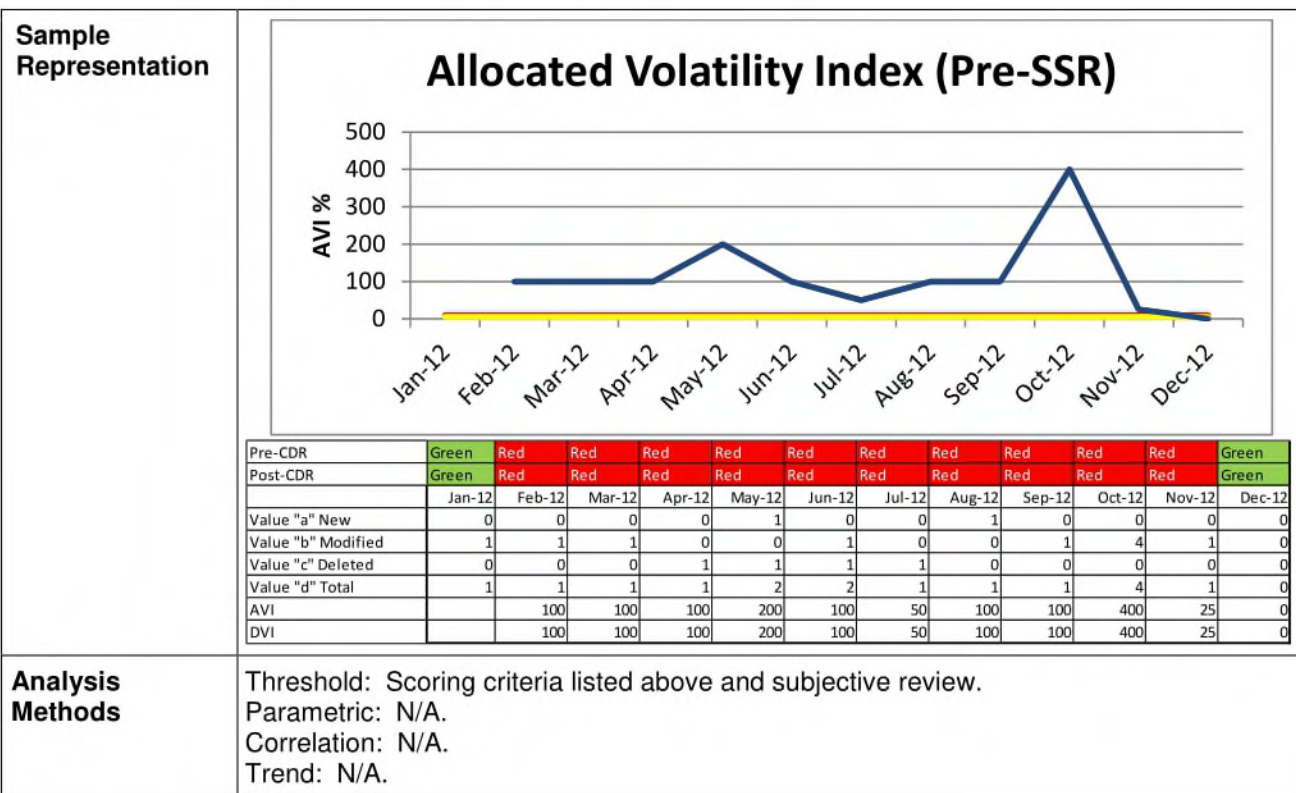
B.4.6.4 Software Interface Stability.

B.4.6.5 Software Functionality Stability.

B.4.6.6 Software Coding Progress.

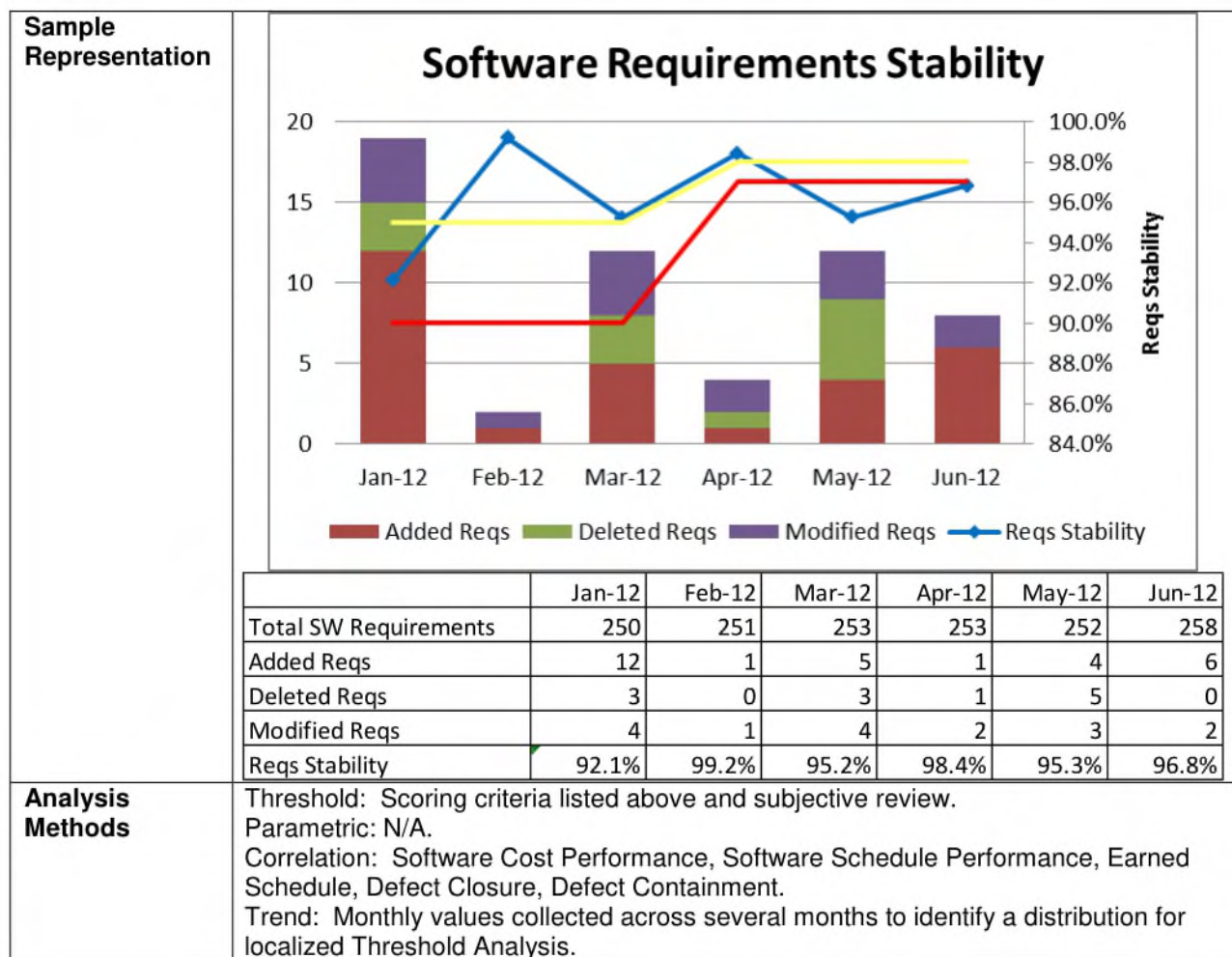
B.4.6.1 Requirements Volatility Index

Description	Requirements Volatility Index is a quantitative measure of changes to baseline requirements. Requirements are in the Hardware Requirements Specification, Software Requirements Specification, and the Interface Requirements Specification.
Critical Area	Growth and Stability
Application	<p>Requirements Volatility is applicable to all MDA programs.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Is there volatility in the allocated system requirements which can lead to rework and additional effort or necessitate a re-plan? Is there volatility in the derived requirements which can lead to rework and additional effort? Are the requirements sufficiently stable so that subsequent development activities can proceed? Is there a need to re-plan based on changes to allocated requirements? Is the program doing a good job in its decomposition of allocated requirements?
Data Primitives Collected	<p>Separately report cumulative hardware, software, and interface component values for allocated and derived requirements at each new document baseline:</p> <ol style="list-style-type: none"> New Modified Deleted Total
Aggregate Values Calculated	<p>For each of the requirements volatility categories (allocated and derived):</p> <ol style="list-style-type: none"> Allocated Volatility Index (AVI) Percentage = $\frac{[(\text{New} + \text{Modified} + \text{Deleted}) / \text{Total of previous baseline}] \times 100}{}$ Derived Volatility Index (DVI) Percentage = $\frac{[(\text{New} + \text{Modified} + \text{Deleted}) / \text{Total of previous baseline}] \times 100}{}$
Scoring Criteria	<p>Volatility Index % value of 0 is optimum. Values > 0 indicate that the program is undergoing capability, function, or requirements churn.</p> <p>Prior to the Software Specification Review (SSR) (3.4.1.5) (report only AVI%):</p> <p>GREEN: < 5%</p> <p>YELLOW: $5\% \leq \text{AVI}\% \leq 10\%$</p> <p>RED: > 10%</p> <p>After the SSR (3.4.1.5) (report AVI% and DVI%):</p> <p>Prior to the [Software/Hardware/Interface] Critical Design Review (CDR) milestone:</p> <p>GREEN: $\text{AVI}\% = 0 \text{ AND } \text{DVI}\% < 5\%$</p> <p>YELLOW: $0\% < \text{AVI}\% \leq 1\% \text{ OR } 5\% \leq \text{DVI}\% \leq 10\%$</p> <p>RED: $\text{AVI}\% > 1\% \text{ OR } \text{DVI}\% > 10\%$</p> <p>After the [Software/Hardware/Interface] CDR milestone:</p> <p>GREEN: $\text{AVI}\% = 0 \text{ AND } \text{DVI}\% < 2\%$</p> <p>YELLOW: $\text{AVI}\% = 0 \text{ AND } 2\% \leq \text{DVI}\% \leq 3\%$</p> <p>RED: $\text{AVI}\% > 0\% \text{ OR } \text{DVI}\% > 3\%$</p>



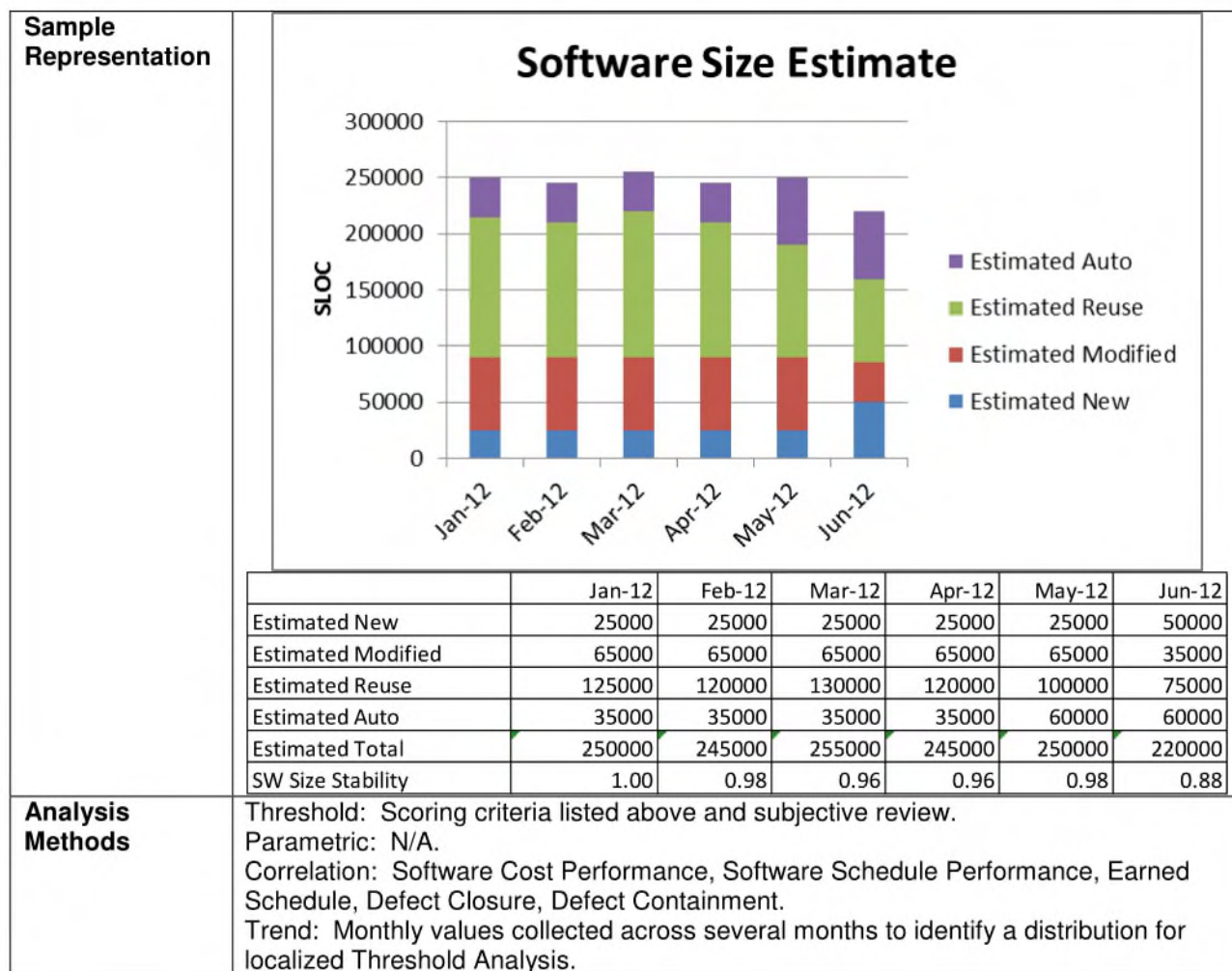
B.4.6.2 Software Requirements Stability

Description	The Software Requirements Stability indicator is used to assess the extent of software requirements ("shall" statements) change over the development of the program. The software requirements stability indicator report captures volatility in the requirements which can lead to unplanned rework and additional effort and cost. Software Requirements Stability is collected at the lowest possible software level (Software Requirement Specifications and Interface Requirement Specifications) for a build.
Critical Area	Growth and Stability
Application	Applicable to all MDA software development programs Collected monthly, by software build and major component from Preliminary Design through Formal Qualification Test. Answers the question: Are the requirements baselined and understood to drive the remainder of software development?
Data Primitives Collected	a. Software Requirements Added (monthly). b. Software Requirements Modified (monthly). c. Software Requirements Deleted (monthly). d. Total Software Requirements (monthly).
Aggregate Values Calculated	Requirements Stability Percentage = $[1 - ((\text{Software Requirements Added} + \text{Modified} + \text{Deleted}) / \text{Total Software Requirements (previous month)})] \times 100$
Scoring Criteria	Requirements Stability GREEN: $\geq 95\%$ [prior to design completion]; $\geq 98\%$ [after design completion] YELLOW: $95\% > \text{Requirements Stability} \geq 90\%$ [prior to design completion]; $98\% > \text{Requirements Stability} \geq 97\%$ [after design completion] RED: $< 90\%$ [prior to design completion]; $< 97\%$ [after design completion]



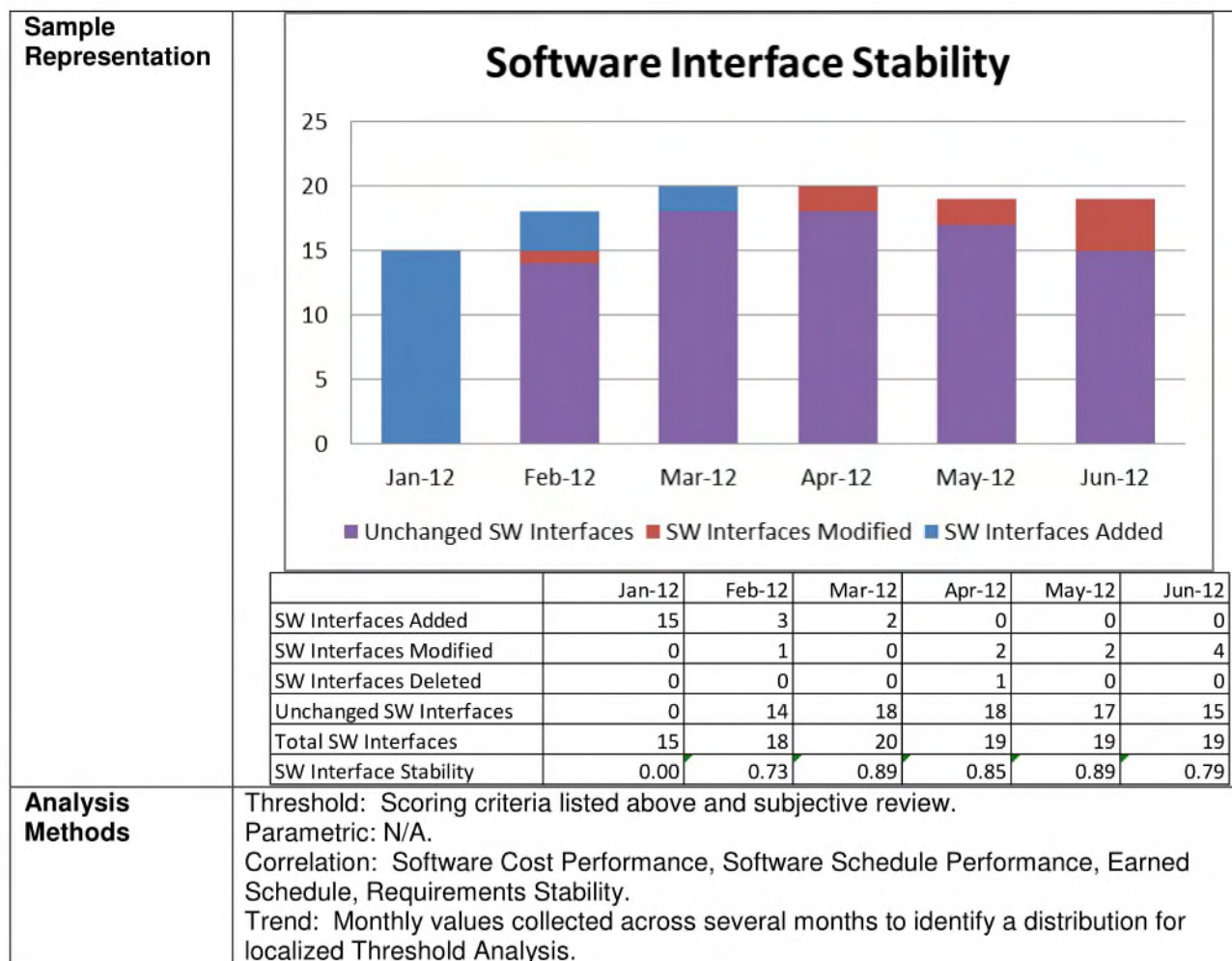
B.4.6.3 Software Size Estimate

Description	This indicator tracks the estimated total size (measured in Source Lines of Code (SLOC)) of the software product to be delivered at completion. A SLOC is defined as a non-comment, non-blank logical line of computer code (typically ending in a semi-colon). Estimates for planned lines of code are updated monthly and plotted to determine trends in code growth or shrinkage. "Reused SLOC" means a software unit or item that is reused in its entirety without modification of a single line of code, thereby preserving its test legacy. "Modified SLOC" is a software unit or item that is reused, but requires changes to the legacy design or code base for integration. "New SLOC" is a software unit or item that is developed completely new, from design through unit testing, requiring a full test effort. Estimated software size is measured to control large changes in effort.
Critical Area	Growth and Stability
Application	Applicable to all MDA software development programs Collected monthly, by software build and major component from Requirements Analysis through Formal Qualification Test. Estimated SLOC is the current, final estimate of software size at project completion. Answers the question: Is the estimated code development accurate and stable?
Data Primitives Collected	a. Estimated New SLOC (monthly). b. Estimated Modified SLOC (monthly). c. Estimated Reuse SLOC (monthly). d. Estimated Auto-Generated SLOC (monthly).
Aggregate Values Calculated	a. Estimated Total SLOC = New + Modified + Reuse + Auto-Generated b. Software Size Stability Percentage = $(1 - (Estimated\ Total\ SLOC\ (current\ month) - Estimated\ Total\ SLOC\ (previous\ month) / (Estimated\ Total\ SLOC\ (previous\ month))) \times 100$
Scoring Criteria	Software Size Stability GREEN: $\geq 90\%$ [prior to design completion]; $\geq 95\%$ [after design completion] YELLOW: $90\% > Requirements\ Stability \geq 75\%$ [prior to design completion]; $95\% > Requirements\ Stability \geq 90\%$ [after design completion] RED: $< 75\%$ [prior to design completion]; $< 90\%$ [after design completion]



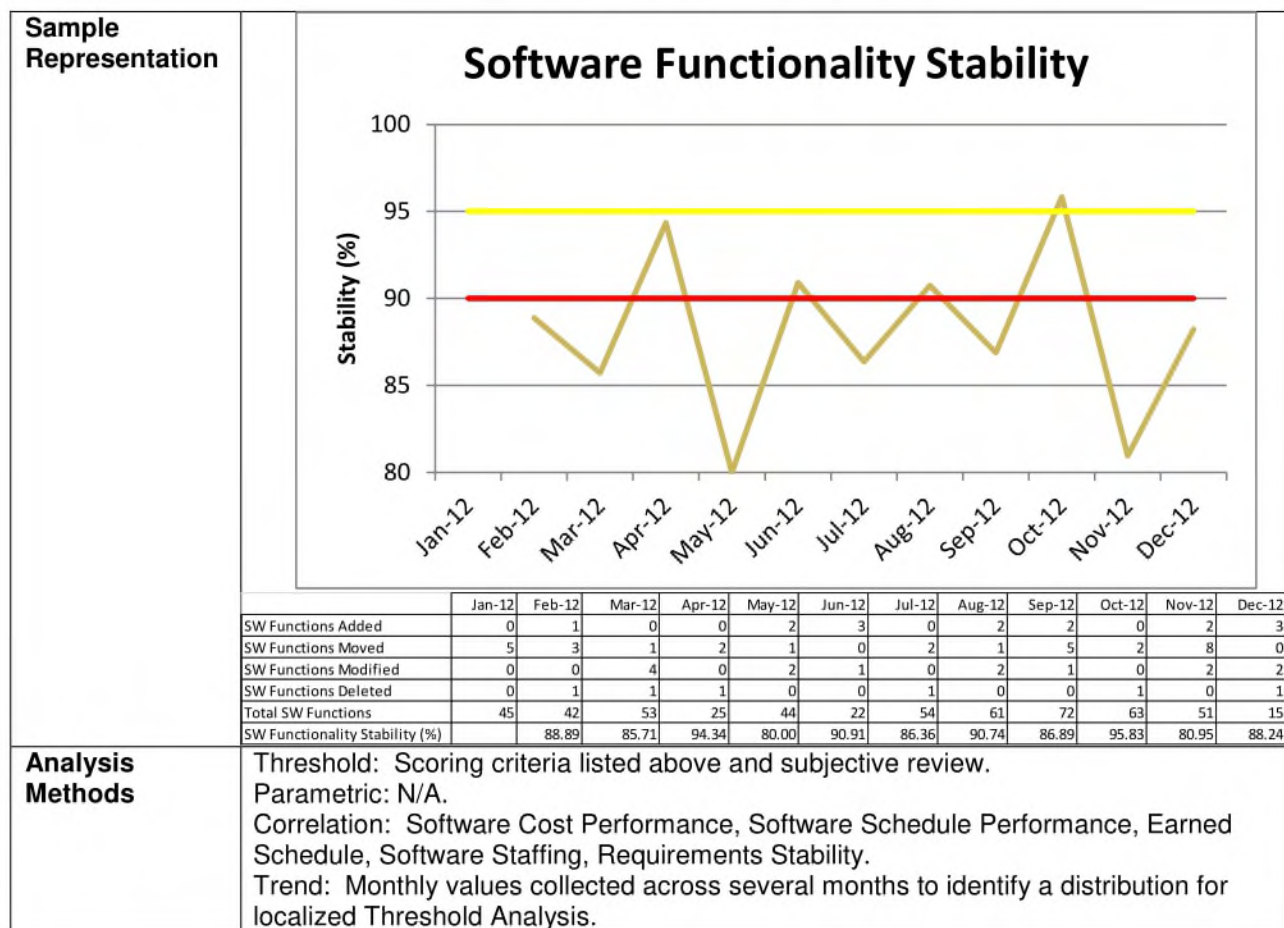
B.4.6.4 Software Interface Stability

Description	This indicator helps assess progress in defining system interfaces and in stabilizing their definitions over time. Software interfaces should be understood and defined once the architecture is defined and understood. Changes to the interfaces after design is complete will lead to unplanned rework and additional cost.
Critical Area	Growth and Stability
Application	Applicable to all MDA software development programs. Collected monthly, by software build and major component from Requirements Analysis through Formal Qualification Test. Answers the question: Are the software interfaces defined and understood?
Data Primitives Collected	a. Software Interfaces Added (monthly). b. Software Interfaces Modified (monthly). c. Software Interfaces Deleted (monthly). d. Unchanged Software Interfaces (monthly).
Aggregate Values Calculated	a. Total Software Interfaces = Added + Modified + Deleted + Unchanged b. Software Interface Stability Percentage = $(1 - (\text{Software Interfaces Added} + \text{Software Interfaces Modified} + \text{Software Interfaces Deleted}) / \text{Total Software Interfaces (previous month)}) \times 100$
Scoring Criteria	Software Interface Stability (only scored post-Preliminary Design Review (PDR)) GREEN: $\geq 95\%$ YELLOW: $95\% > \text{Requirements Stability} \geq 90\%$ RED: $< 90\%$



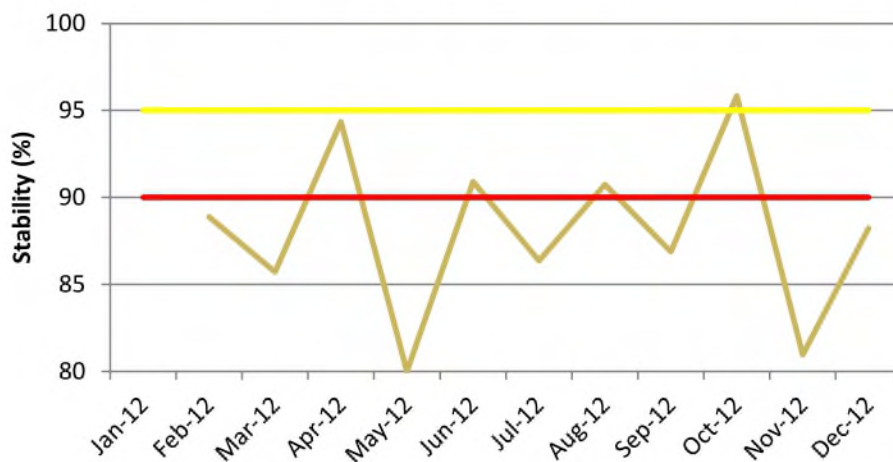
B.4.6.5 Software Functionality Stability

Description	This indicator tracks the software functions as attributed to the software versions that support software builds. As the software build plan and architecture are established, functions are assigned to versions within the build. As these functions are deferred, deleted, or modified, there is a requirement for program management insight into the expected deliveries and the functionality assigned to them.
Critical Area	Growth and Stability
Application	Applicable to all MDA software development programs. Collected monthly, by software build and software version from Requirements Analysis through Formal Qualification Test. It is understood that early in the software life cycle there may not be defined build versions. Answers the question: Is the software functionality stabilized and understood?
Data Primitives Collected	a. List of software functions (by version, monthly). b. Software functions added (monthly). c. Software functions moved (monthly). d. Software functions modified (monthly). e. Software functions deleted (monthly). f. Total software functions (monthly).
Aggregate Values Calculated	Software Functionality Stability Percentage = $1 - ((\text{Software functions added} + \text{moved} + \text{modified} + \text{deleted}) / \text{Total software functions}(\text{previous month})) \times 100$
Scoring Criteria	Software Functionality Stability (only scored post-Preliminary Design Review) GREEN: $\geq 95\%$ YELLOW: $95\% > \text{Software Functionality Stability} \geq 90\%$ RED: $< 90\%$ [after design completion]



Sample Representation

Software Functionality Stability



Analysis Methods

Threshold: Scoring criteria listed above and subjective review.

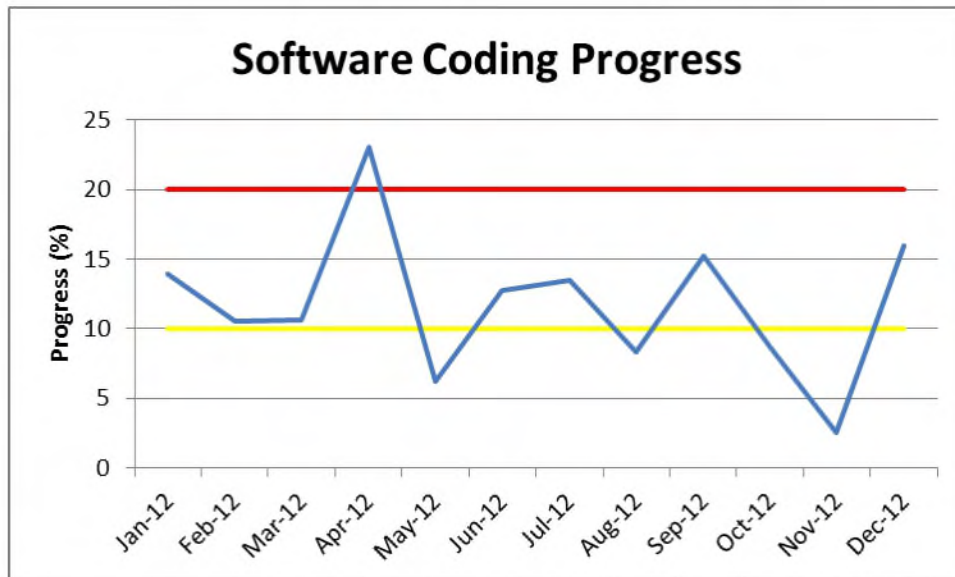
Parametric: N/A.

Correlation: Software Cost Performance, Software Schedule Performance, Earned Schedule, Software Staffing, Requirements Stability.

Trend: Monthly values collected across several months to identify a distribution for localized Threshold Analysis.

B.4.6.6 Software Coding Progress

Description	This metric provides an indication of coding progress against the planned software development schedule. This metric is used as an input to improving software size estimation.
Critical Area	Growth and Stability
Application	Software coding progress is applicable to all MDA software development programs. Answers the question: Is software code development progressing as planned?
Data Primitives Collected	Separately report BMD Element software component monthly values: a. Planned New Code. b. Planned Reuse (modified and unmodified) Code. c. Actual New Code. d. Actual Reuse (modified and unmodified) Code.
Aggregate Values Calculated	a. Total Planned at Completion of Reporting Period Software Size = Value "a" + Value "b" b. Total Actual at Completion of Reporting Period Software Size = Value "c" + Value "d" c. Software Coding Progress Percentage = $((\text{Value "c"} + \text{Value "d"}) / (\text{Value "a"} + \text{Value "b"})) \times 100$
Scoring Criteria	Software Coding Progress Percent GREEN: < 10% YELLOW: $0\% \leq \text{Software Coding Progress Percent} \leq 20\%$ RED: > 20%

**Sample
Representation**

	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Planned New Code	27	15	22	42	22	22	22	33	37	28	34	57
Planned Reuse (modified and unmodified) Code	45	42	25	23	42	33	52	27	22	41	45	18
Actual New Code	0	2	1	4	2	2	6	0	2	2	2	2
Actual Reuse (modified and unmodified) Code	10	4	4	11	2	5	4	5	7	4	0	10
Total Planned at Completion of Reporting Period Software Size	72	57	47	65	64	55	74	60	59	69	79	75
Total Actual at Completion of Reporting Period Software Size	10	6	5	15	4	7	10	5	9	6	2	12
Software Coding Progress Percent	13.88889	10.52632	10.6383	23.07692	6.25	12.72727	13.51351	8.333333	15.25424	8.695652	2.531646	16

**Analysis
Methods**

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

B.4.7 Adequacy, Quality, Safety, and Performance

The area of Adequacy, Quality, Safety, and Performance provides evidence of the extent to which product safely and securely meets program capability requirements and that the delivered product safely and securely meets the user's intention without failure. The indicators in Adequacy, Quality, Safety, and Performance are:

- B.4.7.1 Defect Density.
- B.4.7.2 Defect Profile.
- B.4.7.3 Defect Closure.
- B.4.7.4 Defect Containment.
- B.4.7.5 First Time Quality of Software.
- B.4.7.6 Defect History.
- B.4.7.7 Engineering Change Proposal Cycle Time.
- B.4.7.8 Engineering Change Proposal Approval Rate.
- B.4.7.9 Number of Deviation Requests and Percent Recurring.
- B.4.7.10 Change Incorporation Rate.
- B.4.7.11 Completion of Class I Engineering Change Proposals Implementing Actions.
- B.4.7.12 Rework.
- B.4.7.13 Failure Review Board.
- B.4.7.14 Foreign Object Elimination.
- B.4.7.15 Waivers and Deviations.
- B.4.7.16 MRB Actions, Dispositions, and Cost Metrics.
- B.4.7.17 Occupational Safety.
- B.4.7.18 System Safety Progress.
- B.4.7.19 Software Safety Status.
- B.4.7.20 Inherent Availability.
- B.4.7.21 Operational Availability.
- B.4.7.22 Mean Time To Repair.
- B.4.7.23 Mean Time To Restore Function.
- B.4.7.24 Mean Time Between Critical Failure.
- B.4.7.25 Mean Time Between Critical Failure.

13 June 2014

MDA-QS-001-MAP-Rev B

B.4.7.26 Mean Logistics Delay Time.

B.4.7.27 Mean Repair Time.

B.4.7.28 Fault Detection.

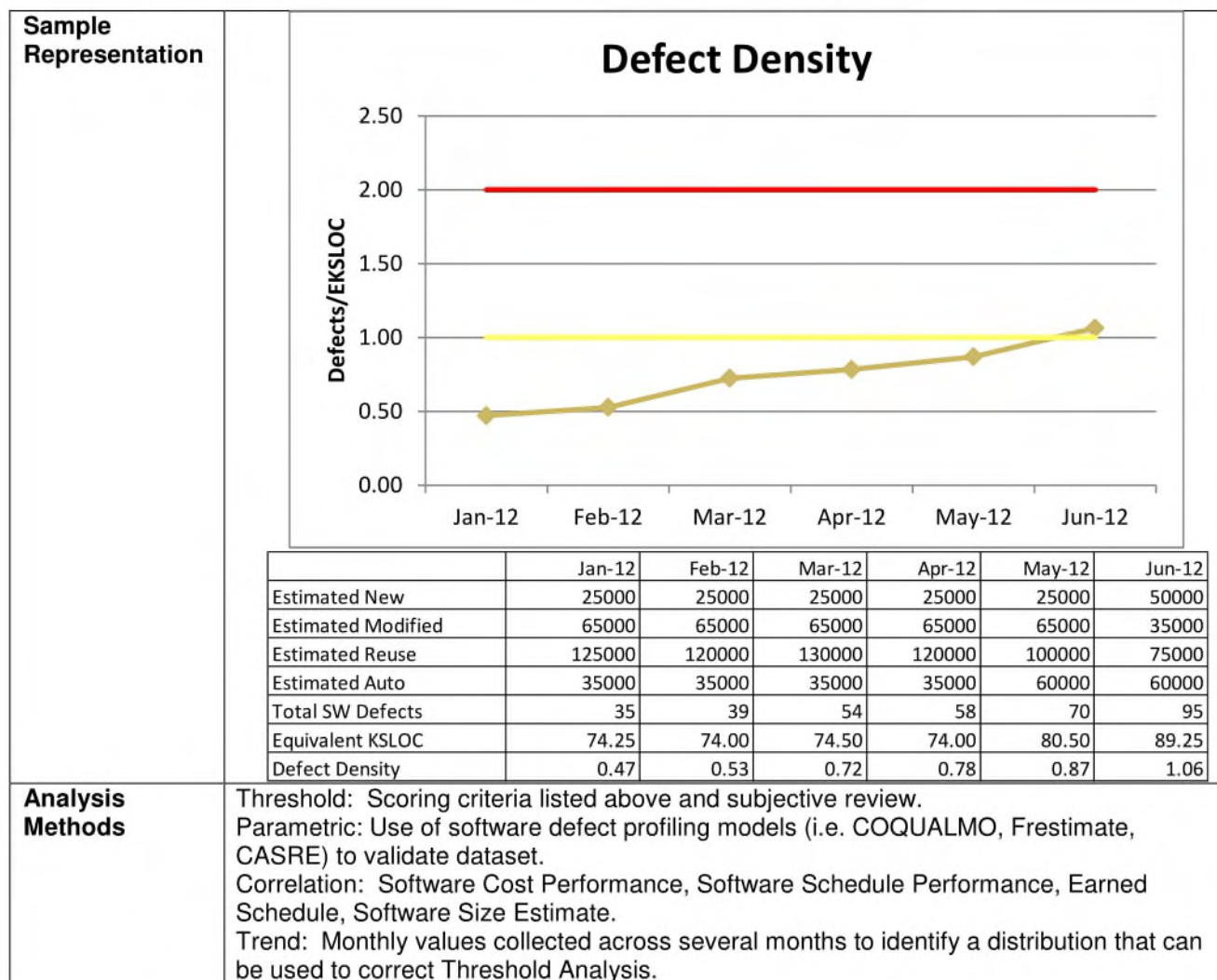
B.4.7.29 Fault Isolation.

B.4.7.30 Maintenance Ratio.

~~For Official Use Only~~

B.4.7.1 Defect Density

Description	The Defect Density indicator report includes the enumeration of defects discovered per estimated Equivalent Thousand Source Lines of Code (EKSLOC) of developed software. Defect density measures software and process quality normalized by the developmental size of the project. Defects are defined as problems in the software or software products that are found outside of the development phase in which they are introduced. These are also commonly referred to as "out-of-phase" defects, since their detection escaped beyond any peer reviews that define the end of development for individual work products. Problems found before or during peer review are defined as errors and are not counted as defects. A defect that causes changes to multiple software products is counted as a single defect.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Applicable to all MDA software development programs Collected monthly, by software build and component from Preliminary Design Review through Formal Qualification Test. Answers the question: Is the software quality sufficient normalized for the size of the effort?
Data Primitives Collected	a. Estimated New SLOC. b. Estimated Modified SLOC. c. Estimated Reuse SLOC. d. Estimated Auto-Generated SLOC. e. Total Software Defects.
Aggregate Values Calculated	a. $\text{Equivalent KSLOC} = ((\text{New}) + (0.5) \times (\text{Modified}) + (0.05) \times (\text{Reuse}) + (0.3) \times (\text{Auto-Generated})) / 1000$ b. $\text{Defect Density} = \text{Total Software Defects} / \text{Equivalent KSLOC}$
Scoring Criteria	Defect Density GREEN: ≤ 1.0 Defects per EKSLOC YELLOW: $1.0 \text{ Defects per EKSLOC} < \text{Defect Density} \leq 2.0 \text{ Defects per EKSLOC}$ RED: $> 2.0 \text{ Defects per EKSLOC}$



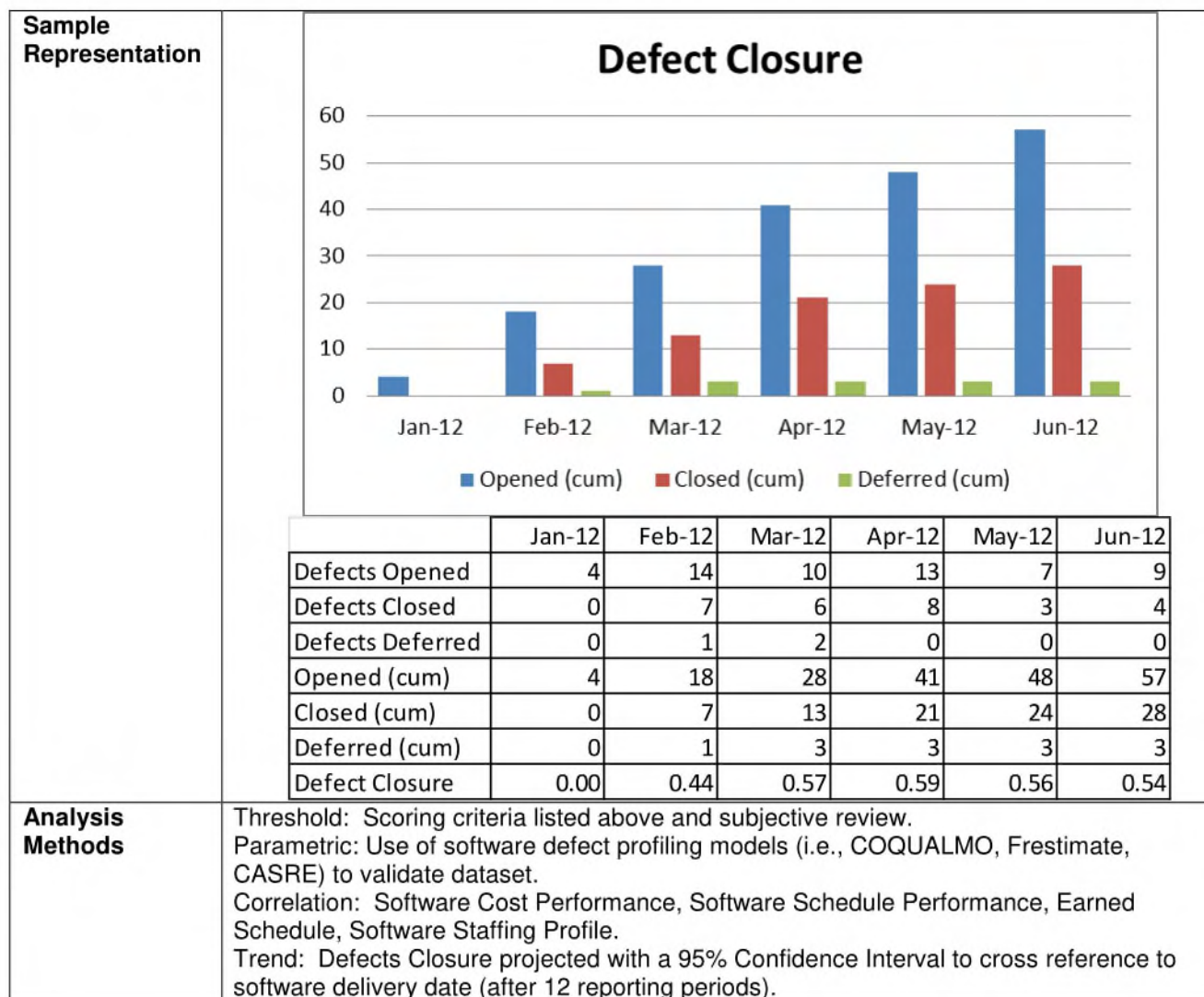
B.4.7.2 Defect Profile

Description	<p>The Defect Profile indicator includes the severity and aging of software defects. Defect Aging identifies defects by the duration in days that they are left in an open state. Defect Severity identifies defects by their individual level of impact to the system. Defect Aging and Severity will be used in concert to identify defects that have not been closed tempered by their system impact. Defect Severity is defined in the five levels below:</p> <p>a. Severity Level 1 (System Abort): Prevents the accomplishment of an operational mission essential capability or jeopardizes safety.</p> <p>b. Severity Level 2 (System Degraded - No Work Around): Adversely affects the accomplishment of an operational or mission essential capability for which no alternative work around solution is known (program restarts/reboots are not acceptable work around solutions).</p> <p>c. Severity Level 3 (System Degraded – Work Around): Adversely affects the accomplishment of an operational or mission essential capability but a work around solution is known.</p> <p>d. Severity Level 4 (System Not Degraded): Results in user/operator inconvenience or annoyance but does not degrade a required operational or mission essential capability.</p> <p>e. Severity Level 5 (Minor Change): Any other change is classified as severity level 5. Many documentation changes are considered severity level 5.</p>																														
Critical Area	Adequacy, Quality, Safety, and Performance																														
Application	<p>Applicable to all MDA software development programs.</p> <p>Collected monthly, by software build and component from Preliminary Design Review through Sustainment.</p> <p>Answers the questions:</p> <p>a. Are software defects being addressed in a timely manner?</p> <p>b. Are severe software defects being corrected in a timely manner?</p> <p>c. What is the severity of the remaining software defects in the program?</p>																														
Data Primitives Collected	<p>a. Software Defects Severity Level [1, 2, 3, 4, 5] Open <= 30 Days</p> <p>b. Software Defects Severity Level [1, 2, 3, 4, 5] Open 31-60 Days</p> <p>c. Software Defects Severity Level [1, 2, 3, 4, 5] Open 61-90 Days</p> <p>d. Software Defects Severity Level [1, 2, 3, 4, 5] Open > 90 Days</p>																														
Aggregate Values Calculated	Total Open Defects Level [1, 2, 3, 4, 5] = ∑ Software Defects Open by Level across Aging categories																														
Scoring Criteria	<p>Defect Profile</p> <p>YELLOW: 2 ≥ Total Open Severity 1 > 0 10 ≥ Total Open Severity 2 or 3 > 5</p> <p>RED: Total Open Severity 1 > 2 Total Open Severity 2 or 3 > 10</p> <p>Defect Profile</p> <table><tr><td></td><td>≤ 30 Days</td><td>31-60 Days</td><td>61-90 Days</td><td>> 90 Days</td></tr><tr><td>Severity 1</td><td></td><td></td><td></td><td></td></tr><tr><td>Severity 2</td><td></td><td></td><td></td><td></td></tr><tr><td>Severity 3</td><td></td><td></td><td></td><td></td></tr><tr><td>Severity 4</td><td></td><td></td><td></td><td></td></tr><tr><td>Severity 5</td><td></td><td></td><td></td><td></td></tr></table>		≤ 30 Days	31-60 Days	61-90 Days	> 90 Days	Severity 1					Severity 2					Severity 3					Severity 4					Severity 5				
	≤ 30 Days	31-60 Days	61-90 Days	> 90 Days																											
Severity 1																															
Severity 2																															
Severity 3																															
Severity 4																															
Severity 5																															

Sample Representation		≤ 30 Days	31-60 Days	61-90 Days	> 90 Days	Total
	Severity 1	0	0	0	0	0
	Severity 2	1	1	0	0	2
	Severity 3	7	2	1	0	10
	Severity 4	14	2	3	0	19
	Severity 5	20	12	0	0	32
Analysis Methods	Threshold: Scoring criteria listed above and subjective review					
	Parametric: Use of software defect profiling models (i.e., COQUALMO, Frestimate, CASRE) to validate dataset.					
	Correlation: Software Cost Performance, Software Schedule Performance, Earned Schedule, Software Size Estimate, Software Staffing Profile.					
	Trend: Monthly values collected across several months to identify a distribution that can be used to correct Threshold Analysis.					

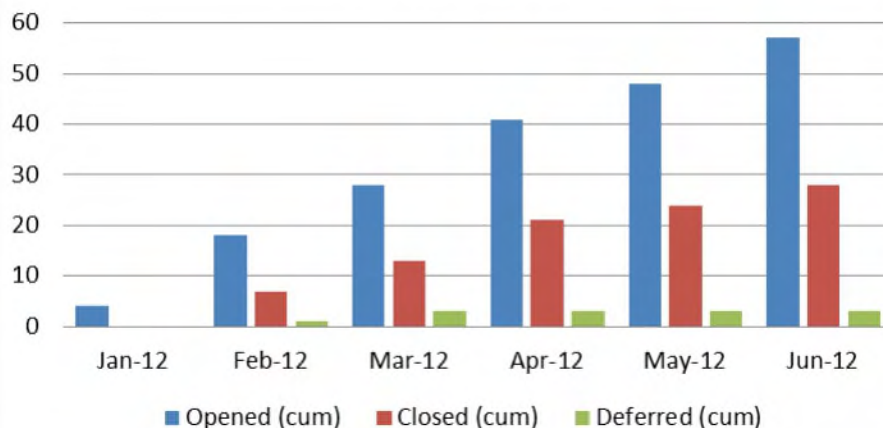
B.4.7.3 Defect Closure

Description	The defect closure indicator includes the defects opened and closed in the developed software. Defect closure measures software and process quality as a function of the rate of closure of defects. Defect closure rate is a preliminary indicator of the effectiveness and availability of resources for product quality.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Applicable to all MDA software development programs. Collected monthly, by software build and component from Preliminary Design Review through Sustainment. Answers the questions: a. Are software defects being addressed and closed? b. How many known defects remain in the software product?
Data Primitives Collected	a. Software Defects Opened (monthly, cumulative). b. Software Defects Closed (monthly, cumulative). c. Software Defects Deferred (monthly, cumulative).
Aggregate Values Calculated	Defect Closure Percentage = $((\text{Defects Closed (cumulative)} + \text{Defects Deferred (cumulative)}) / \text{Defects Opened (cumulative)}) \times 100$
Scoring Criteria	Defect Closure GREEN: Defect Closure $\geq 80\%$ YELLOW: $80\% > \text{Defect Closure} \geq 70\%$ RED: Defect Closure $< 70\%$



Sample Representation

Defect Closure



Analysis Methods

Threshold: Scoring criteria listed above and subjective review.
 Parametric: Use of software defect profiling models (i.e., COQUALMO, Frestimate, CASRE) to validate dataset.
 Correlation: Software Cost Performance, Software Schedule Performance, Earned Schedule, Software Staffing Profile.
 Trend: Defects Closure projected with a 95% Confidence Interval to cross reference to software delivery date (after 12 reporting periods).

B.4.7.4 Defect Containment

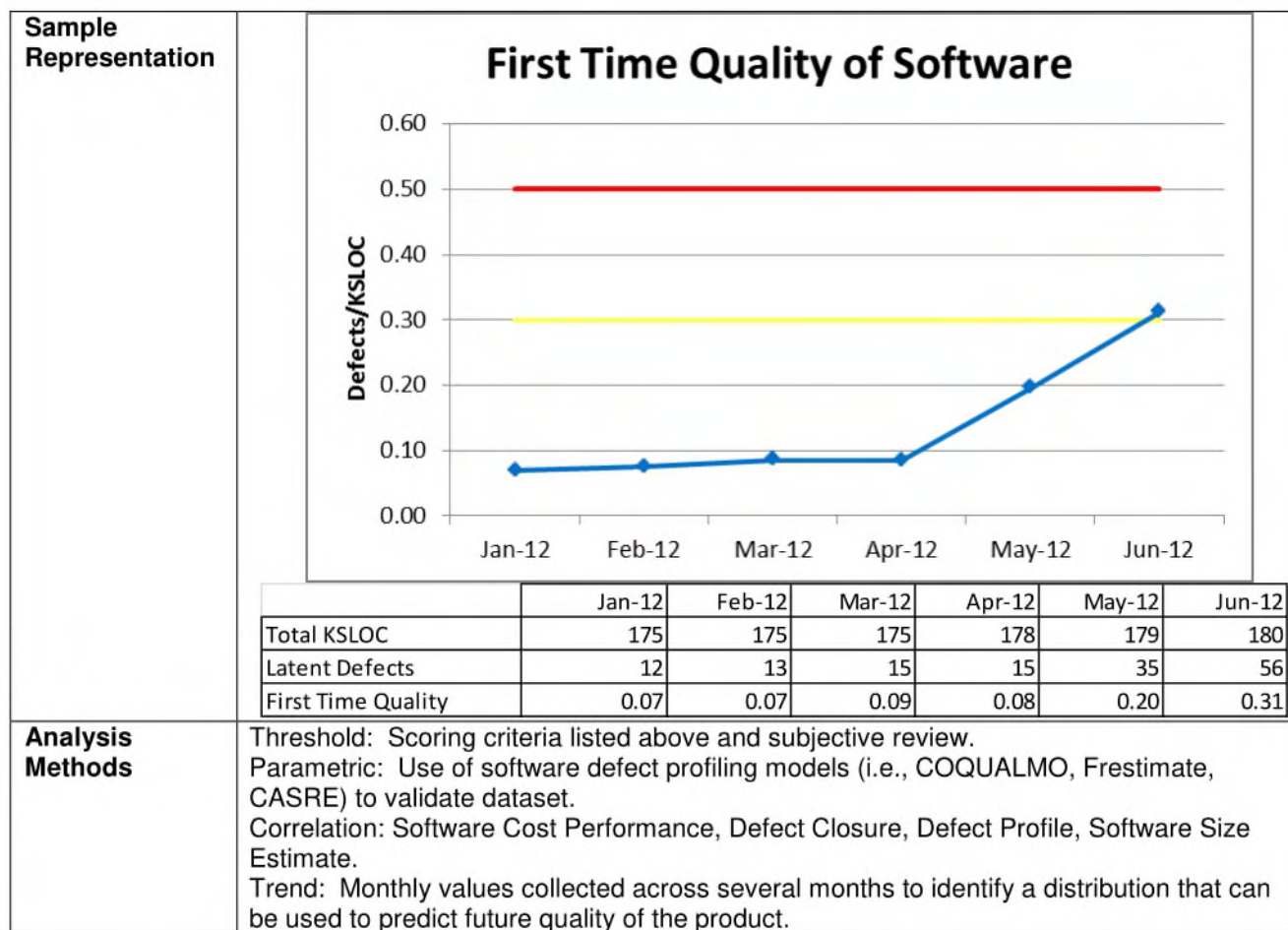
Description	<p>The defect containment indicator classifies defects by phase of inception and phase of detection. Problems that are detected "outside of phase" can increase correction costs at a geometric level, increasing for each phase that the defect goes undetected. Defect Containment is used to identify "leakage" of defects and impacts to cost (rework) and quality. Here, a defect is a problem injected in one life cycle phase and detected in a later phase. A problem injected and detected in the same phase is an error.</p> <p>The assumed life cycle phases for the software development are Requirements Analysis, Preliminary Design, Critical Design, Code and Unit Testing, Integration and Testing, Software Formal Qualification Test, and Post Release.</p>
Critical Area	Adequacy, Quality, Safety, and Performance
Application	<p>Applicable to all MDA software development programs.</p> <p>Collected monthly, by software build and component from Requirements Analysis through sustainment.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Are latent defects being reduced? Are defects being fixed closer to their origin?
Data Primitives Collected	<ol style="list-style-type: none"> Errors found by phase detected. Requirements Analysis defects by phase detected. Preliminary Design defects by phase detected. Detailed Design defects by phase detected. Code and Unit Testing defects by phase detected. Integration and Testing defects by phase detected. Software Formal Qualification Test defects by phase detected.
Aggregate Values Calculated	<ol style="list-style-type: none"> Total Containment Effectiveness (TCE) Percentage = $(\sum \text{Defects (pre-release)} + \sum \text{Errors}) / (\sum \text{Defects (pre and post-release)} + \sum \text{Errors}) \times 100$ Phase Containment Effectiveness (PCE)* Percentage = $\text{Errors (phase)} / (\text{Errors (phase)} + \text{Defects (phase)}) \times 100$ Defect Containment Effectiveness (DCE)** Percentage = $\text{Defects (phase)} / (\text{Defects (phase)} + \sum \text{Defects (downstream phases)}) \times 100$ <p><i>* Phase Containment Effectiveness is used to measure how successful the defect containment process at a single phase is at finding errors before they become defects. The PCE is collected individually by phase from Preliminary Design through Integration and Testing.</i></p> <p><i>** Defect Containment Effectiveness is used to measure how successful the defect containment process at a single phase is at finding defects that are passed to it. The DCE is collected individually by phase from Detailed Design through Software Formal Qualification Test.</i></p>
Scoring Criteria	<p>Defect Containment</p> <p>GREEN: TCE \geq 95%</p> <p>YELLOW: 95% > Defect Closure \geq 75%</p> <p>RED: Defect Closure < 75%</p>

Sample Representation	Product Phases	Phase Found											
		Planning	System Requirements	System Design	Prelim. Design	Detail Design	Implementation	Integration and Test	System Integration and Test	Formal system Verification	Operation Test Validation	Production and Deployment	Operation and Support
Phase Injected	Planning	1	2										
	System Requirements		0		5	2							
	System Design			1									
	Preliminary Design				3								
	Detailed Design					12	2						
	Implementation						0						
	Integration and Test							2	2	2			
	System Integration and Test								4				
	Formal system Verification									0			
	Operation Test Validation										0		1
	Production and Deployment											0	
	Operation and Support												0
	% Detected in-phase	100%	0%	100%	38%	86%	0%	100%	67%	0%	0%	0%	0%
	Month	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
	Total Out-of-Phase	0	0	0	5	2	2	0	2	2	0	0	1
	Total Found	1	3	4	12	26	28	30	36	38	38	38	39

Analysis Methods	Threshold: Scoring criteria listed above and subjective review.
	Parametric: N/A.
	Correlation: N/A.
	Trend: N/A.

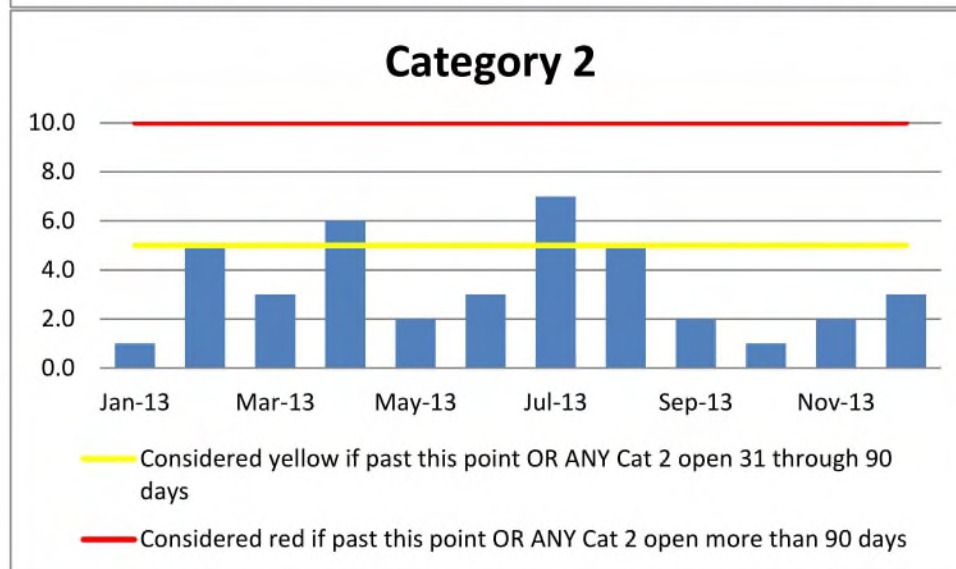
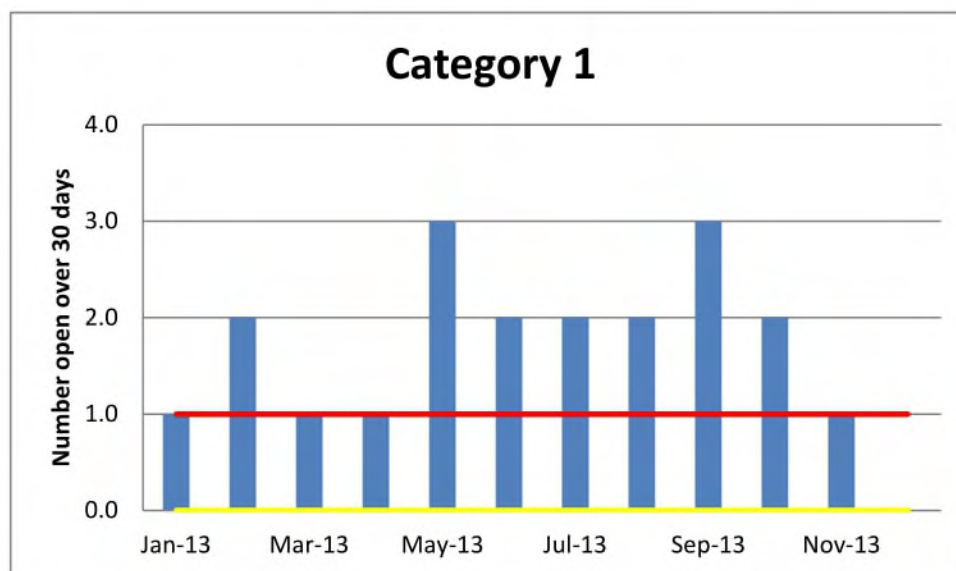
B.4.7.5 First Time Quality of Software

Description	The First Time Quality of Software indicator tracks the project's ability to effectively transform software product requirements into accurate product definition data. This metric represents the quality of submitted software products with respect to required content, effective review, and compliance to requirements. This is done by measuring the quantity of latent software defects on released software as a function of thousands of lines of code developed. As opposed to Defect Density, First Time Quality of Software focuses on Total Delivered Source Lines of Code (SLOC) and Post Release software defects.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Applicable to all MDA software development programs. Collected monthly, by software build during Post Release. Answers the question: What is the quality of the software that has been delivered and accepted?
Data Primitives Collected	a. Actual Total Delivered SLOC (monthly). b. Latent Defects (cumulative, Post Release).
Aggregate Values Calculated	First Time Quality of Software = Latent Defects / Actual Total Delivered SLOC
Scoring Criteria	First Time Quality of Software GREEN: ≤ 0.3 YELLOW: $0.3 < \text{First Time Quality} \leq 0.5$ RED: > 0.5

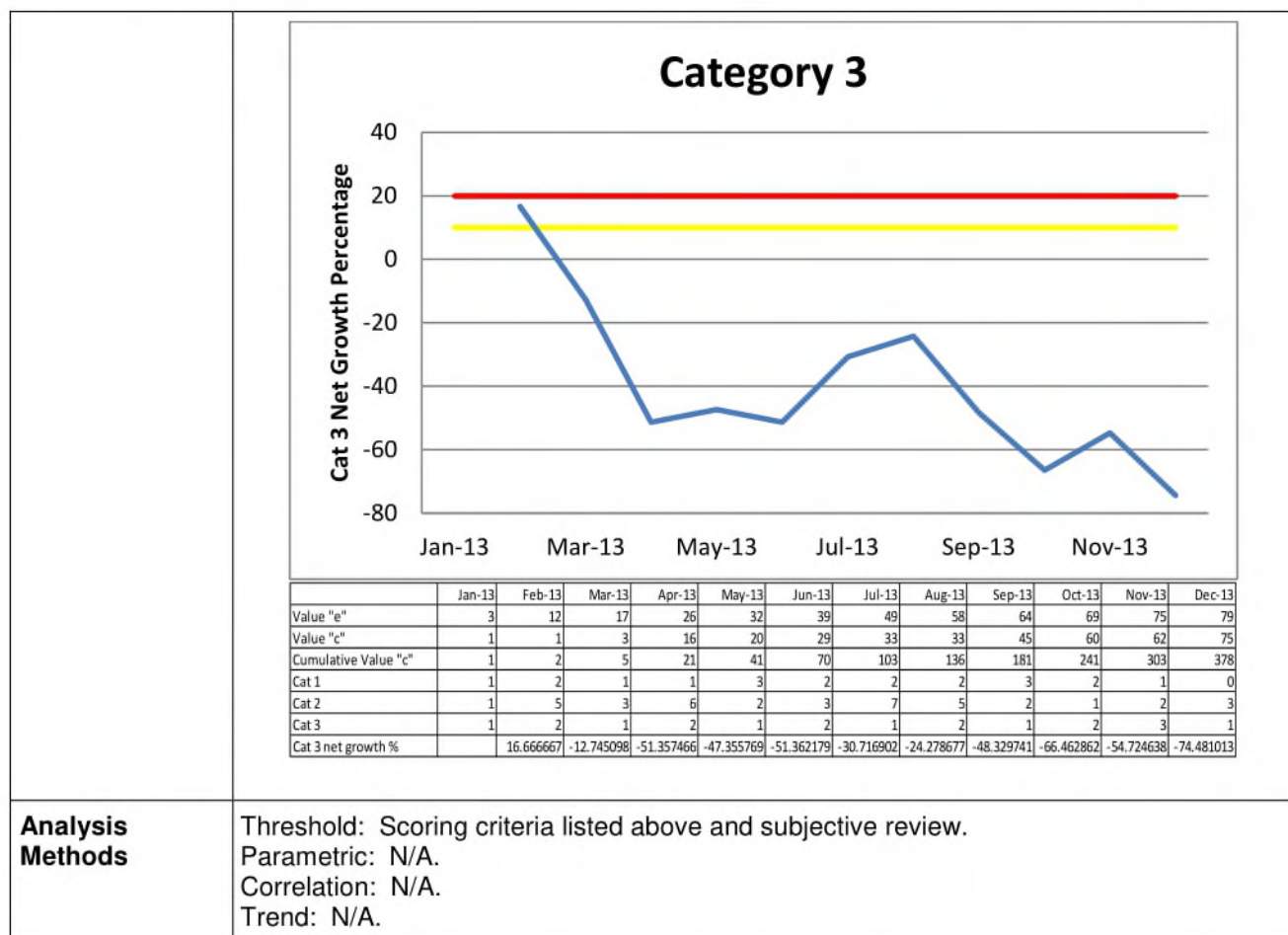


B.4.7.6 Defect History

Description	Defect History provides a quantitative measure of progress in resolving identified system and hardware defects. Defect History identifies the number of defects opened, resolved, closed, and deferred by criticality level.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	<p>Defect History is applicable to all MDA programs. Defect History is used to assess defect closure cycle time, number of Category 1, Category 2, and Category 3 defects, and identify potential closure problems.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Are there identified Category 1, Category 2, and Category 3 defects in the product? Are identified Category 1, Category 2, and Category 3 defects being resolved within a reasonable time? What is the total number of identified defects in the product to date?
Data Primitives Collected	<p>Separately report system, hardware, and component defect values by Category 1, Category 2, and Category 3 *.</p> <ol style="list-style-type: none"> Number newly opened (current period). Number resolved (i.e., fix identified but not implemented or verified) (current and cumulative). Number closed (i.e., fix implemented and verified) (current and cumulative). Number remaining open (current period): <ol style="list-style-type: none"> 0-30 days 31-60 days 61-90 days >90 days Total number of identified defects to date by system and hardware. <p>*Category 1 (Critical): A critical defect impacts safety or results in failure of a system, subsystem, or component. Category 2 (Major): A major defect results in failure or degradation of an end item to perform a required function. This includes impacts on occupational health, performance, interchangeability, reliability, survivability, or maintainability. Category 3 (Minor): A defect not classified as a critical or major.</p>
Aggregate Values Calculated	<p><i>Category 3 Net Open Growth Percent</i></p> $= \left[\text{Current Period} \left(\frac{\text{Value } e - \text{Cumulative Value } c}{\text{Value } e} \right) \right] \times 100$ $- \left[\text{Previous Period} \left(\frac{\text{Value } e - \text{Cumulative Value } c}{\text{Value } e} \right) \right] \times 100$
Scoring Criteria	<p>Scoring Criteria for defects open:</p> <p>GREEN: Category 1 in an open state = 0 days Category 2 in an open state < 5 days Category 3 Net Open Growth Percent <10%</p> <p>YELLOW: Any Category 1 open ≤ 30 days 5 days < = Category 2 in an open state ≤ 10 days OR any Category 2 opened 31 through 90 days 10% ≤ Category 3 Net Open Growth Percent ≤ 20%</p> <p>RED: Category 1 open > 30 days Category 2 >10 or any Category 2 opened more than 90 days Category 3 Net Open Growth Percent >20%</p>

**Sample
Representation**


	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Oct-13	Nov-13	Dec-13
Value "e"	3	12	17	26	32	39	49	58	64	69	75	79
Value "c"	1	1	3	16	20	29	33	33	45	60	62	75
Cumulative Value "c"	1	2	5	21	41	70	103	136	181	241	303	378
Cat 1	1	2	1	1	3	2	2	2	3	2	1	0
Cat 2	1	5	3	6	2	3	7	5	2	1	2	3
Cat 3	1	2	1	2	1	2	1	2	1	2	3	1
Cat 3 net growth %		16.666667	-12.745098	-51.357466	-47.355769	-51.362179	-30.716902	-24.278677	-48.329741	-66.462862	-54.724638	-74.481013

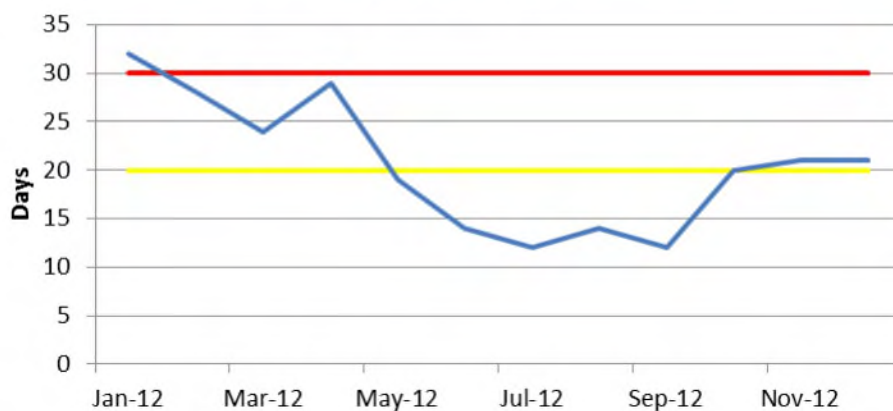
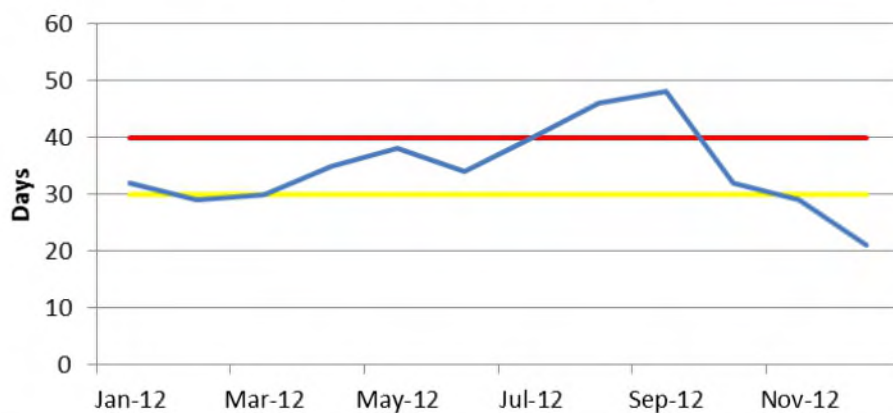


Analysis Methods

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

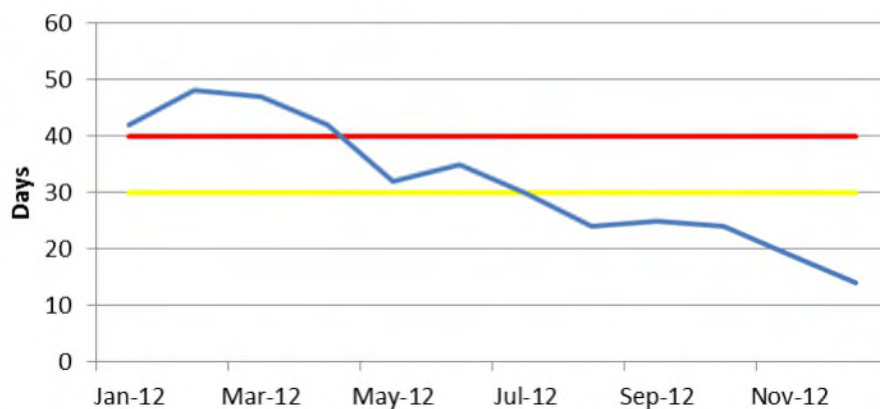
B.4.7.7 Engineering Change Proposal Cycle Time

Description	Shows total time spent in Engineering Change Proposal (ECP) Cycle and which portions of the ECP cycle are the longest. Focuses attention on ECP processing, and highlights areas of inefficient process or insufficient priority. It also isolates contributing factors and constraints, concentrates improvement effort where it will benefit the entire process, and shows the effectiveness of improvements measured over time.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Applicable to all MDA development programs. This data may be stratified by ECP \$ value, complexity factors, ECP Priority codes, or ECP Justification codes to determine the influence of such factors on processing time. Answers the questions: a. What are the constraints for ECP cycle time? b. Are the necessary resources available?
Data Primitives Collected	a. Count of Class I Engineering Change Requests. b. Average Cycle time for Class I Engineering Change Request approvals. c. Average Cycle time for incorporating and verifying approved Class I Engineering Change Requests. d. Count of Class II Engineering Change Requests. e. Average Cycle time for Class II Engineering Change Request approvals. f. Average Cycle time for incorporating and verifying approved Class II Engineering Change Requests.
Aggregate Values Calculated	None required for this metric
Scoring Criteria	<p>Class I Engineering Change Requests</p> <p>GREEN: Class I < 5 Average Cycle Time for Approvals < 20 days Average Cycle Time for Incorporation < 30 days</p> <p>YELLOW: $5 \leq \text{Class I} \leq 10$ $20 \leq \text{Average Cycle Time for Approvals} < 30 \text{ days}$ $30 \leq \text{Average Cycle Time for Incorporation} < 40 \text{ days}$</p> <p>RED: Class I > 10 Average Cycle Time for Approvals > 30 days Average Cycle Time for Incorporation > 40 days</p> <p>Class II Engineering Change Requests</p> <p>GREEN: Class II < 10 Average Cycle Time for Approvals < 30 days Average Cycle Time for Incorporation < 40 days</p> <p>YELLOW: $10 \leq \text{Class II} \leq 20$ $30 \leq \text{Average Cycle Time for Approvals} \leq 40 \text{ days}$ $40 \leq \text{Average Cycle Time for Incorporation} < 50 \text{ days}$</p> <p>RED: Class II > 20 Average Cycle Time for Approvals > 40 days Average Cycle Time for Incorporation > 50 days</p>

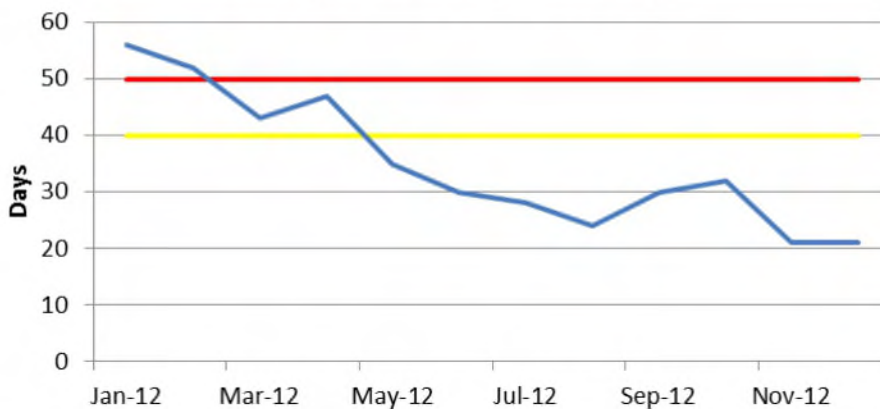
Sample
Representation**Ave. ECP Cycle Time for Approvals
(Class I)****Ave. ECP Cycle Time for
Incorporation (Class I)**

	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Average ECP Cycle Time for Approvals Class I	32	28	24	29	19	14	12	14	12	20	21	21
Average ECP Cycle Time for Incorporation Class I	32	29	30	35	38	34	40	46	48	32	29	21

Ave. ECP Cycle Time for Approvals (Class II)



Ave. ECP Cycle Time for Incorporation (Class II)



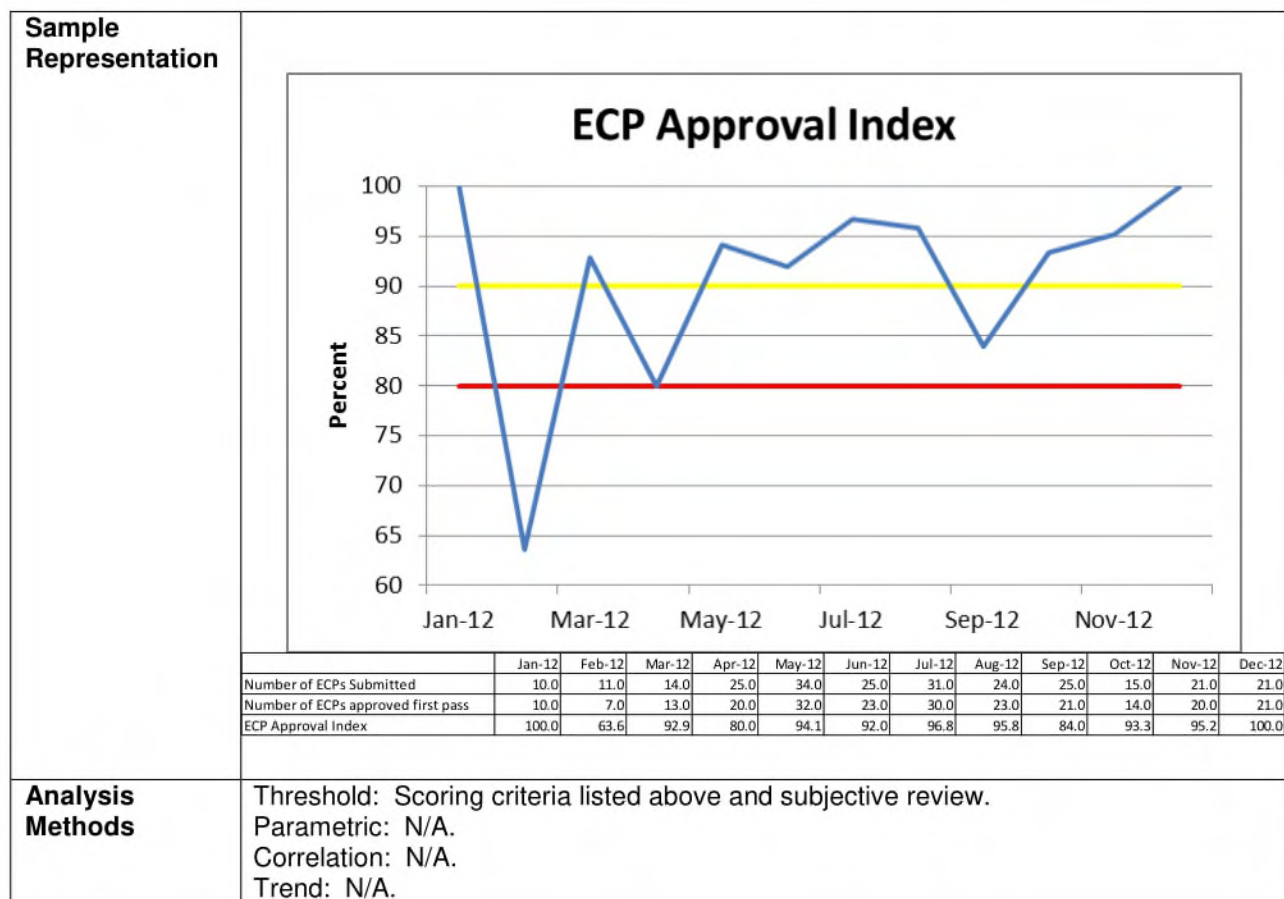
	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Average ECP Cycle Time for Approvals Class II	42	48	47	42	32	35	30	24	25	24	19	14
Average ECP Cycle Time for Incorporation Class II	56	52	43	47	35	30	28	24	30	32	21	21

Analysis Methods

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

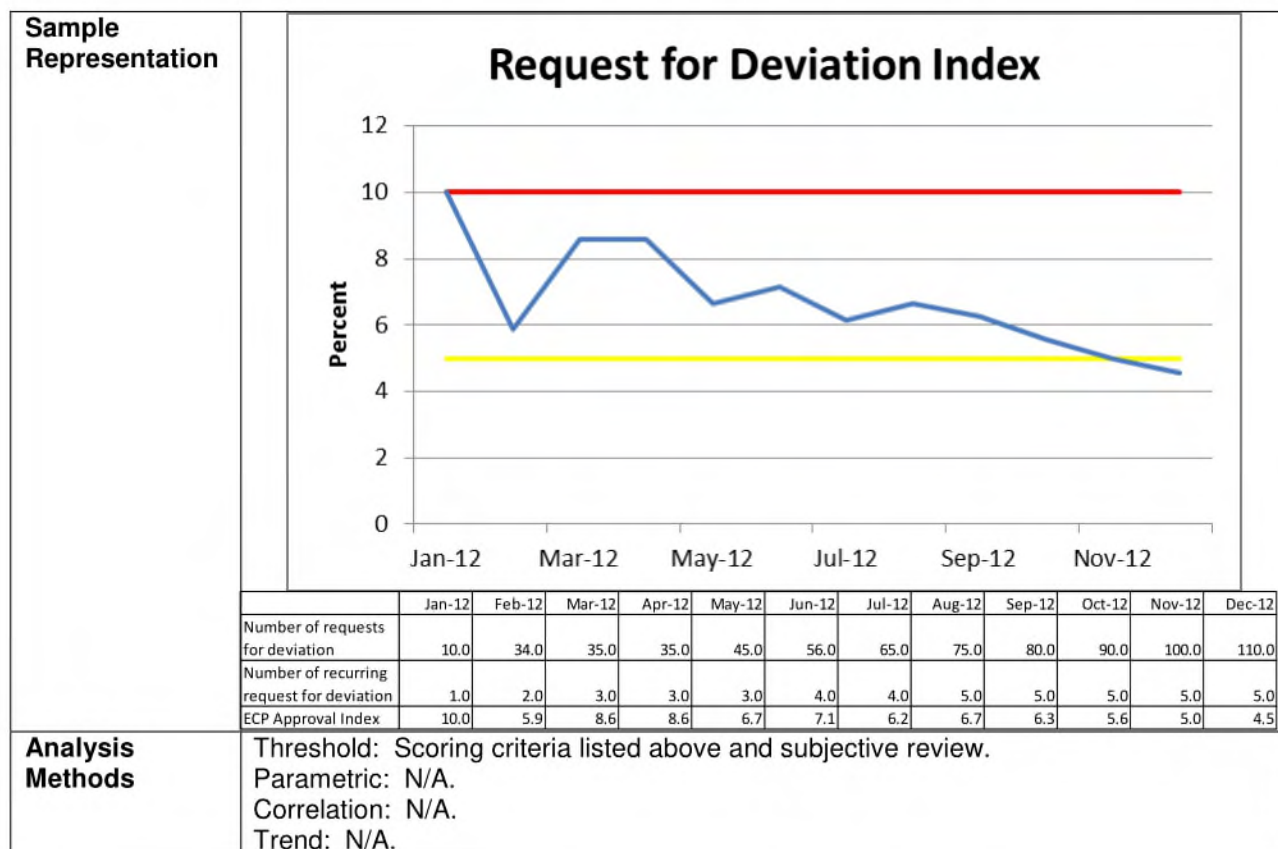
B.4.7.8 Engineering Change Proposal Approval Rate

Description	To obtain a measure of the rate of first pass Engineering Change Proposal (ECP) approvals in any time period.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Applicable to all MDA development programs. Collected monthly or quarterly depending on change volume. Answers the question: Is there an efficient and timely process for submittal and approval of ECPs?
Data Primitives Collected	a. Number of ECPs submitted (monthly and cumulative). b. Number of ECPs approved on First Pass (monthly and cumulative).
Aggregate Values Calculated	<i>First Pass ECP Approval Index Percentage</i> $= \frac{\text{Number of ECPs approved (cumulative)}}{\text{Number of ECPs submitted (cumulative)}} \times 100$
Scoring Criteria	First Pass ECP Approval Index Percentage GREEN: > 90% YELLOW: 90% ≥ First Pass ECP Approval Index ≥ 80% RED: < 80%



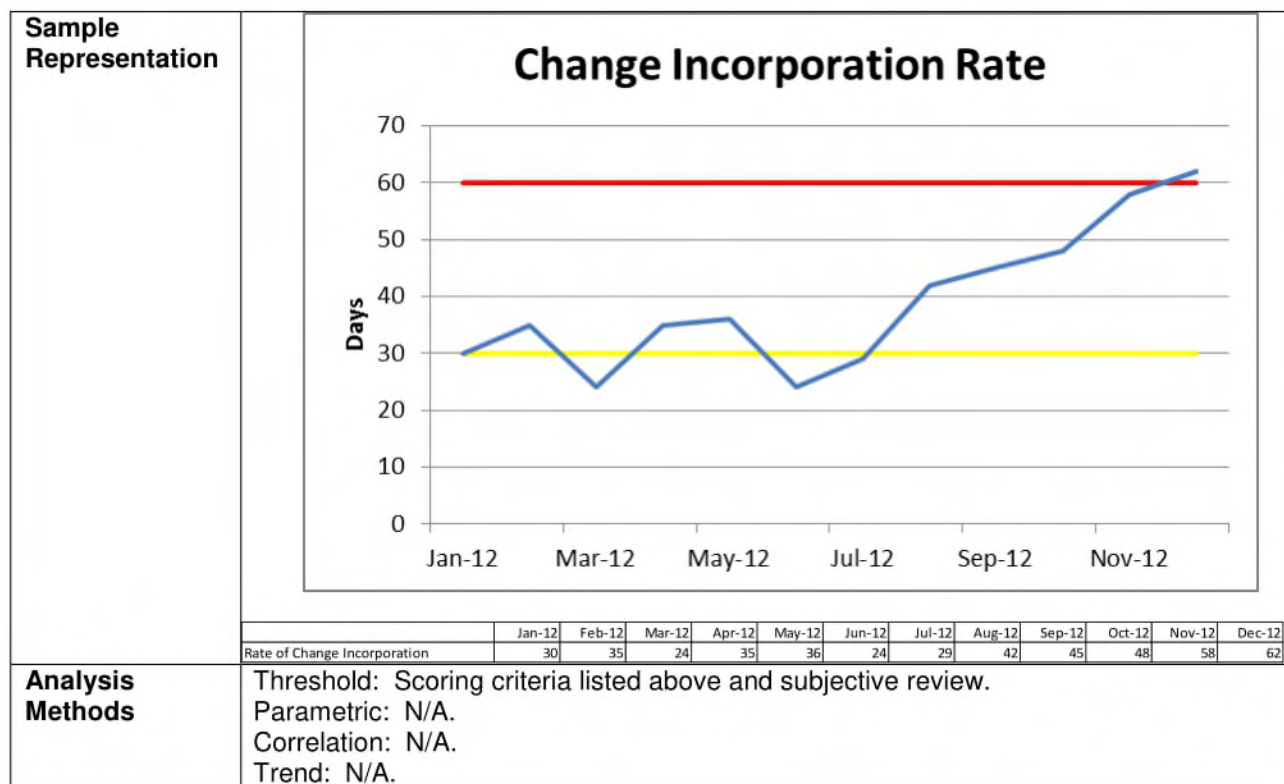
B.4.7.9 Number of Deviation Requests and Percent Recurring

Description	This metric determines and isolates causes of recurring deviation requests.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Applicable to all MDA development programs. Collected monthly. Answers the questions: a. What are the technical areas contributing to the most requests for deviation? b. What percentage of requests for deviation is recurring?
Data Primitives Collected	a. Number of requests for deviation (monthly and cumulative). b. Number of recurring requests for deviation (monthly and cumulative). c. Root cause for requests for deviation.
Aggregate Values Calculated	<i>Request for Deviation Index Percentage</i> $= \frac{\text{Number of recurring requests for deviation (cumulative)}}{\text{Number of requests for deviation (cumulative)}} \times 100$
Scoring Criteria	Request for Deviation Index Percentage GREEN: <5% YELLOW: 10%< Request for Deviation Index ≤ 5% RED: ≥10%



B.4.7.10 Change Incorporation Rate

Description	This metric measures the detailed change activity to be accomplished prior to delivery of each configuration item (rate of incorporation).
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Applicable to all MDA development programs. Collected monthly for each Configuration Item. Answers the question: What is the estimated time for incorporating changes?
Data Primitives Collected	a. Number of new changes being released. b. Time for changes to be verified as completed (monthly and cumulative).
Aggregate Values Calculated	None
Scoring Criteria	Rate of change incorporation GREEN: ≤30 days YELLOW: >30 but ≤60 days RED: >60 days



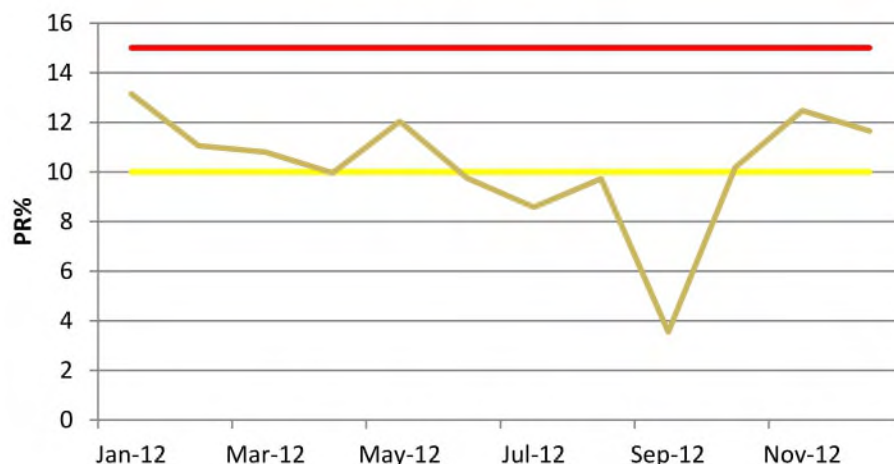
B.4.7.11 Completion of Class I Engineering Change Proposals Implementing Actions

Description	This metric focuses attention on the detailed actions that must be completed to implement an Engineering Change Proposal (ECP) in all areas that are impacted by the ECP.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Applicable to all MDA development programs. Collected monthly. Answers the question: What products are impacted by the ECP and the ECP implementation schedule?
Data Primitives Collected	a. ECP by number. b. Areas affected by ECP. c. Action and responsible organization for completion. d. Schedule for completion. e. Status.
Aggregate Values Calculated	None
Scoring Criteria	Tabular representation of data.

Sample Representation	ECP Number	Action	Response	Sched	Status
	21564	CI	Incorporated	9-17-12	Closed
	21565	SE	Incorporated	8-24-12	Closed
	21566	Pubs	Incorporated	8-30-12	Closed
	21567	Pubs	In work	10-5-12	Open
	21568	SE	Drawing Wait	11-1-12	Open
	21569	SE	In work	12-1-12	Open
	21570	CI	In Work	12-1-12	Open
Analysis Methods	Threshold: Scoring criteria listed above and subjective review. Parametric: N/A. Correlation: N/A. Trend: N/A.				

B.4.7.12 Rework

Description	Rework is that effort associated with bringing contractors' items, products, or materials back into compliance once they are found to be incomplete or not in conformance.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	<p>Rework is applicable to all MDA programs.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> What percent of effort is utilized to correct or change products (intermediate or final) once they are found to be incomplete or not in conformance? How accurately was rework estimated?
Data Primitives Collected	<p>Separately report hardware and software component values, monthly and cumulative:</p> <ol style="list-style-type: none"> Planned Rework effort. Actual Rework effort. Total effort (Actual effort for all developmental activities). Report effort in unit of measure (e.g., hours or dollars). <p>Note: Absence of Planned Rework effort is the same as zero planned rework effort, and will be treated as such in calculating Rework Planning Index.</p>
Aggregate Values Calculated	<p>For hardware and software component values report:</p> <ol style="list-style-type: none"> Percent Rework (PR) = (Value "b" / Value "c") × 100 Rework Planning Index (RPI) = (Value "a" – Value "b") / (Value "a" + Value "b")
Scoring Criteria	<p>Percent Rework:</p> <p>GREEN: <10%</p> <p>YELLOW: 10% ≤ PR ≤ 15%</p> <p>RED: >15%</p> <p>Rework Planning Index:</p> <p>GREEN: -10 < RPI < 10</p> <p>YELLOW: -15 ≤ RPI ≤ -10 or 10 ≤ RPI ≤ 15</p> <p>RED: RPI < -15 or RPI > 15</p>

**Sample
Representation**
Percent Rework

Rework Planning Index


	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Planned Rework effort (dollars)	74000.00	58944.00	101233.00	74000.00	88888.00	75564.00	45768.00	45688.00	22263.00	65422.00	78552.00	98221.00
Actual Rework effort (dollars)	66425.00	57854.00	123565.00	56000.00	78451.00	65854.00	42512.00	47265.00	18566.00	55212.00	65425.00	99524.00
Total Effort (Actual effort for all developmental activities) (dollars)	505101.00	523115.00	1144544.00	562455.00	652128.00	675212.00	495211.00	485611.00	523551.00	542111.00	524511.00	854441.00
Percent Rework (PR)%	13.15	11.06	10.80	9.96	12.03	9.75	8.58	9.73	3.55	10.18	12.47	11.65
Rework Planning Index (RPI)	5.39	0.93	-9.93	13.85	6.24	6.87	3.69	-1.70	9.05	8.46	9.12	-0.66

**Analysis
Methods**

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

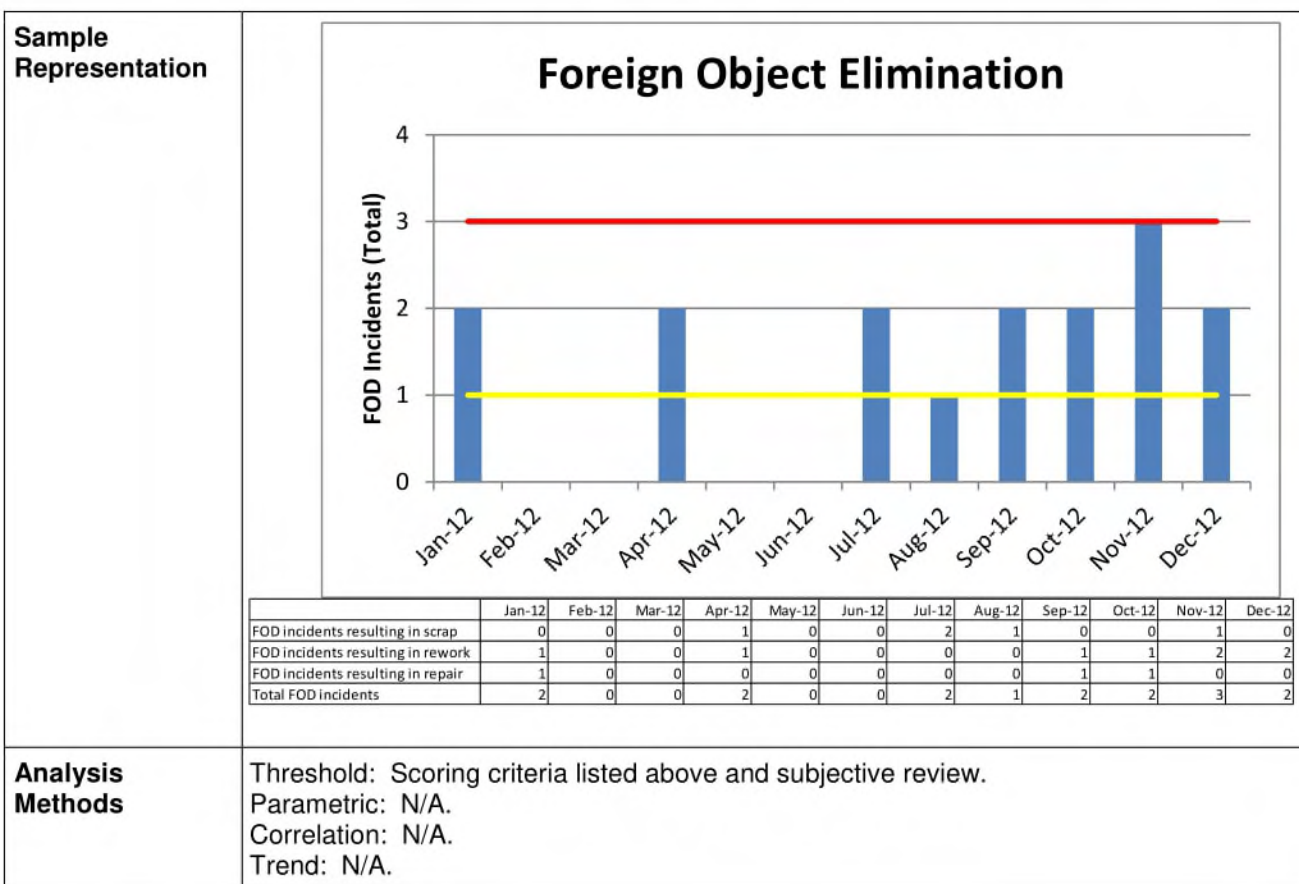
B.4.7.13 Failure Review Board

Description	Failure Review Board (FRB) Progress provides a quantitative measure of progress in monitoring and resolving failure of hardware and software items.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	FRB Progress is applicable to all MDA programs. Answers the questions: a. Have there been any product failures? b. How many failures are being resolved within a reasonable time?
Data Primitives Collected	Separately report hardware and software failure values for Category 1, Category 2, and Category 3 *: a. Number newly opened (current period). b. Number resolved (i.e., fix identified but not implemented or verified) (current and cumulative). c. Number deferred (i.e., fix that has been transferred to later release, build, phase, or spiral) (current and cumulative). d. Number closed (i.e., fix implemented and verified) (current and cumulative). e. Number remaining opened (current period): 1. 0-30 days 2. 31-60 days 3. 61-90 days 4. >90 days f. Total number of identified failures to date. g. Failure root cause. * Category 1 (Catastrophic): A failure, which can cause death or system loss (e.g., aircraft, satellite, missile, or ship). Category 2 (Critical): A failure, which may cause severe injury, major property damage, or major system damage, which will result in mission loss. Category 3 (Minor): A failure, which may cause system degradation or performance loss.
Aggregate Values Calculated	$\begin{aligned} & \text{Category 3 Net Open Growth Percent} \\ &= \left[\text{Current Period} \left(\frac{(\text{Value } f - \text{Cumulative Value } d)}{\text{Value } f} \right) \right] \times 100 \\ & - \left[\text{Previous Period} \left(\frac{(\text{Value } f - \text{Cumulative Value } d)}{\text{Value } f} \right) \right] \times 100 \end{aligned}$
Scoring Criteria	<p>Scoring Criteria for open failures:</p> <p>GREEN: All Category 1 and Category 2 in an open state with FRB-approved Corrective Action Plan, and Category 3 Net Open Growth Percent < 5%</p> <p>YELLOW: Any Category 1 or Category 2 in an open state without FRB-approved Corrective Action Plan for ≤ 30 days, and 5% ≤ Category 3 Net Open Growth Percent ≤ 15%</p> <p>RED: Any Category 1 or Category 2 in an open state without FRB-approved Corrective Action Plan > 30 days, or Category 3 Net Open Growth Percent >15%</p>

Sample Representation		Green	Green	Yellow	Yellow	Yellow	Red	Green	Green	Green	Green	Green	Yellow
		Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
	Value "f"	2	3	3	3	3	3	3	3	3	3	3	3
	Value "d"	1	2	5	6	1	8	9	9	9	9	9	9
	Cumulative Value "d"	1	3	8	14	15	23	32	41	50	59	68	77
	Cat 1	1	0	1	0	0	0	0	0	2	2	1	0
	Cat 2	1	0	3		2	3	0	0	0	1	2	3
	Cat 3 net growth %	#VALUE!	-50	-166.66667	-200	-33.333333	-266.66667	-300	-300	-300	-300	-300	-300
	Analysis Methods	Threshold: Scoring criteria listed above and subjective review.											
Parametric: N/A.													
Correlation: N/A.													
Trend: N/A.													

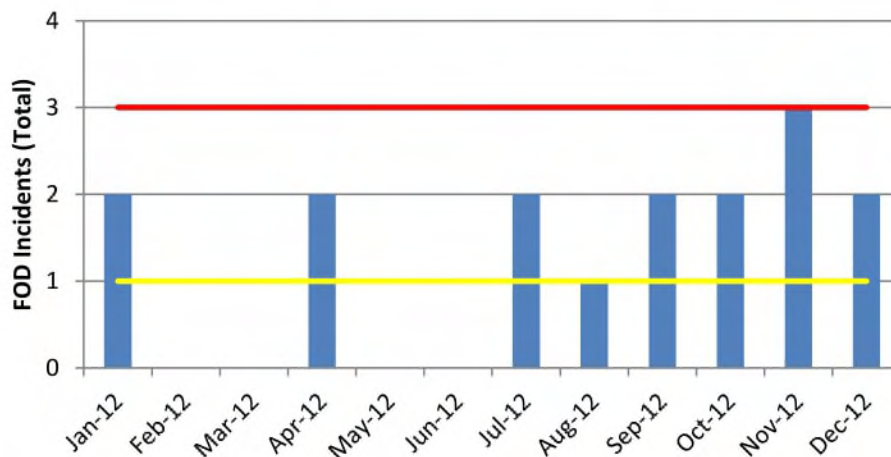
B.4.7.14 Foreign Object Elimination

Description	Foreign Object Elimination provides an indication of the number of Foreign Object Damage and Debris incidents. Foreign Object Damage (FOD) relates to incidents resulting in scrap, rework, or repair.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Foreign Object Elimination is applicable to all MDA hardware development and fabrication activities. Answers the question: How many incidents involving foreign objects occurred?
Data Primitives Collected	Separately report 12-month cumulative value at the BMD Element system and component level for: a. FOD Incidents resulting in scrap. b. FOD incidents resulting in rework. c. FOD incidents resulting in repair.
Aggregate Values Calculated	Total FOD incidents = Value "a" + Value "b" + Value "c"
Scoring Criteria	Total FOD incidents: GREEN: = 0 YELLOW: $1 \leq \text{Total FOD} \leq 3$ RED: > 3



Sample Representation

Foreign Object Elimination

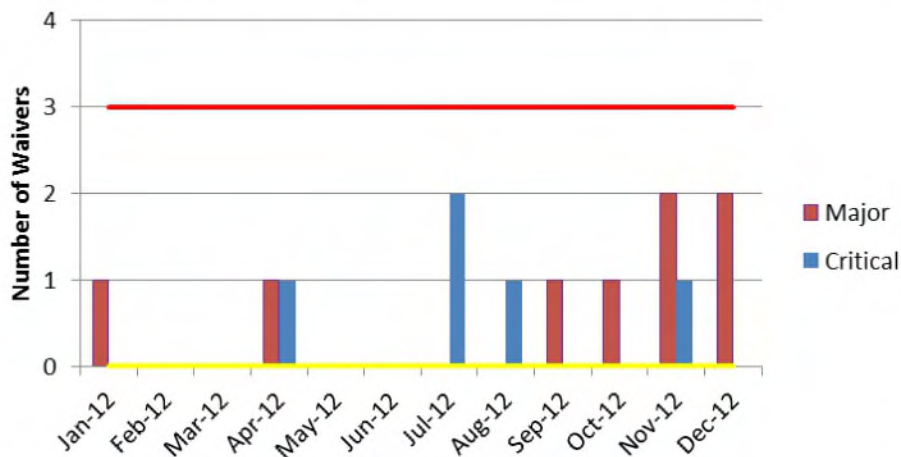
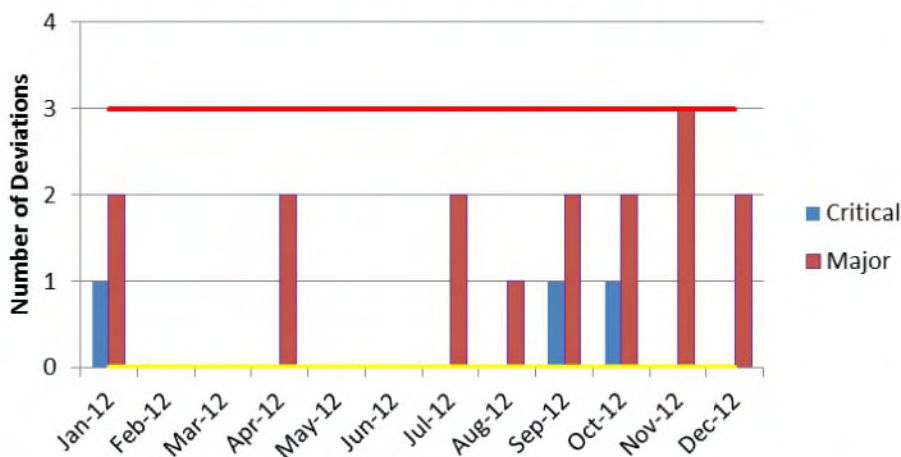


Analysis Methods

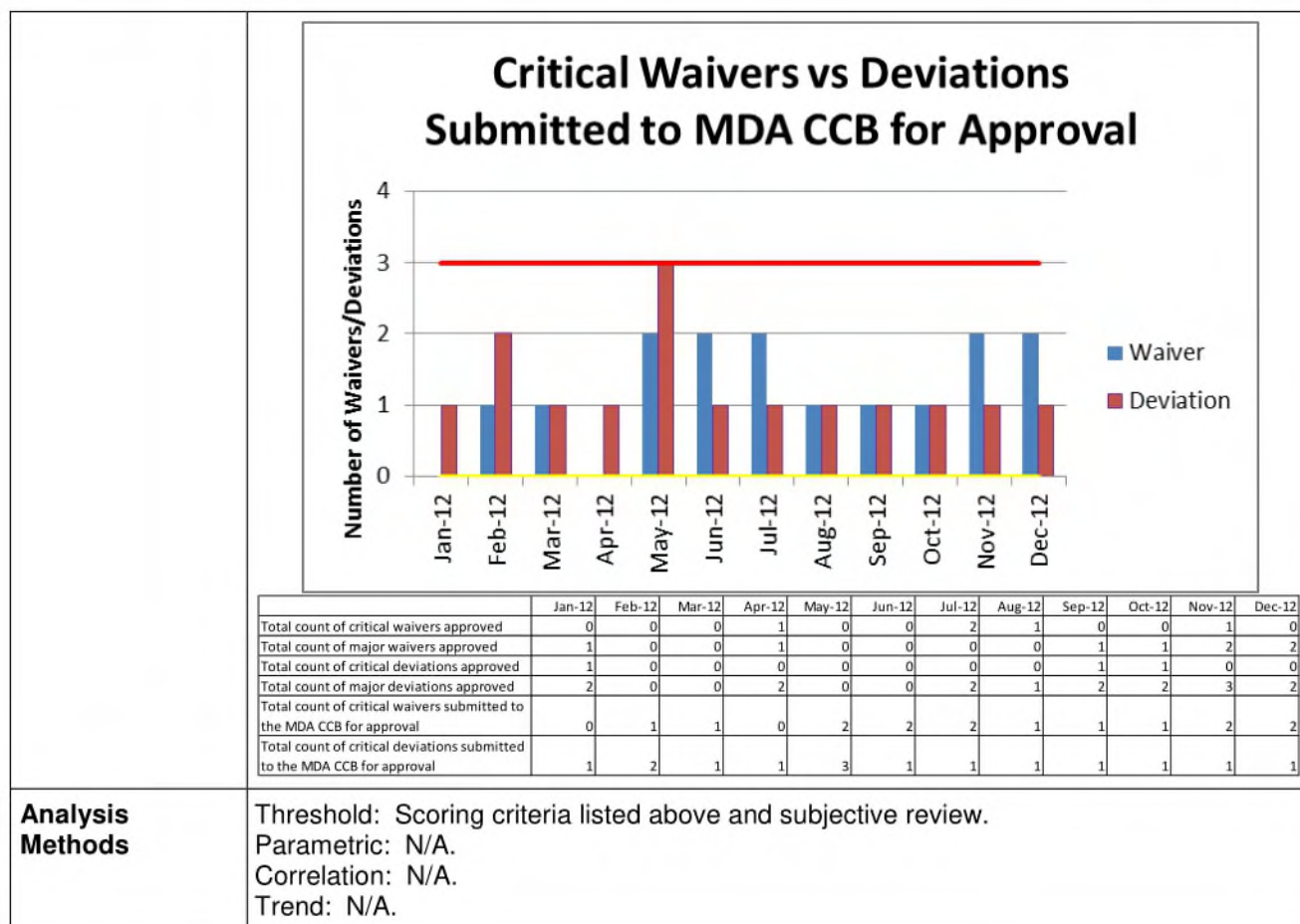
Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

B.4.7.15 Waivers and Deviations

Description	Waivers and Deviations provide an indication of severity and number of departures from contractual requirements or specifications. Waivers grant specification relief after producing a product or component while deviations grant specification relief prior to producing a product or component. Waivers and deviations may be granted for both hardware and software.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	<p>Waivers and Deviations are applicable to all MDA programs.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> How many waivers from contractual requirements or specifications have been approved? How many deviations from contractual requirements or specifications have been approved?
Data Primitives Collected	<p>For each hardware and software component, report the following monthly and cumulative values:</p> <ol style="list-style-type: none"> Total count of Critical waivers approved. Total count of Major waivers approved. Total count of Critical deviations approved. Total count of Major deviations approved. Total count of Critical waivers submitted to the MDA Configuration Control Board (CCB) for approval. Total count of Critical deviations submitted to the MDA CCB for approval.
Aggregate Values Calculated	There are no computation methods for this metric.
Scoring Criteria	<p>Waivers and Deviation Scoring Criteria:</p> <p>GREEN: Critical Waivers or Deviations = 0</p> <p>YELLOW: Critical Waivers or Deviations ≤ 3</p> <p>RED: Critical Waivers or Deviations > 3</p>

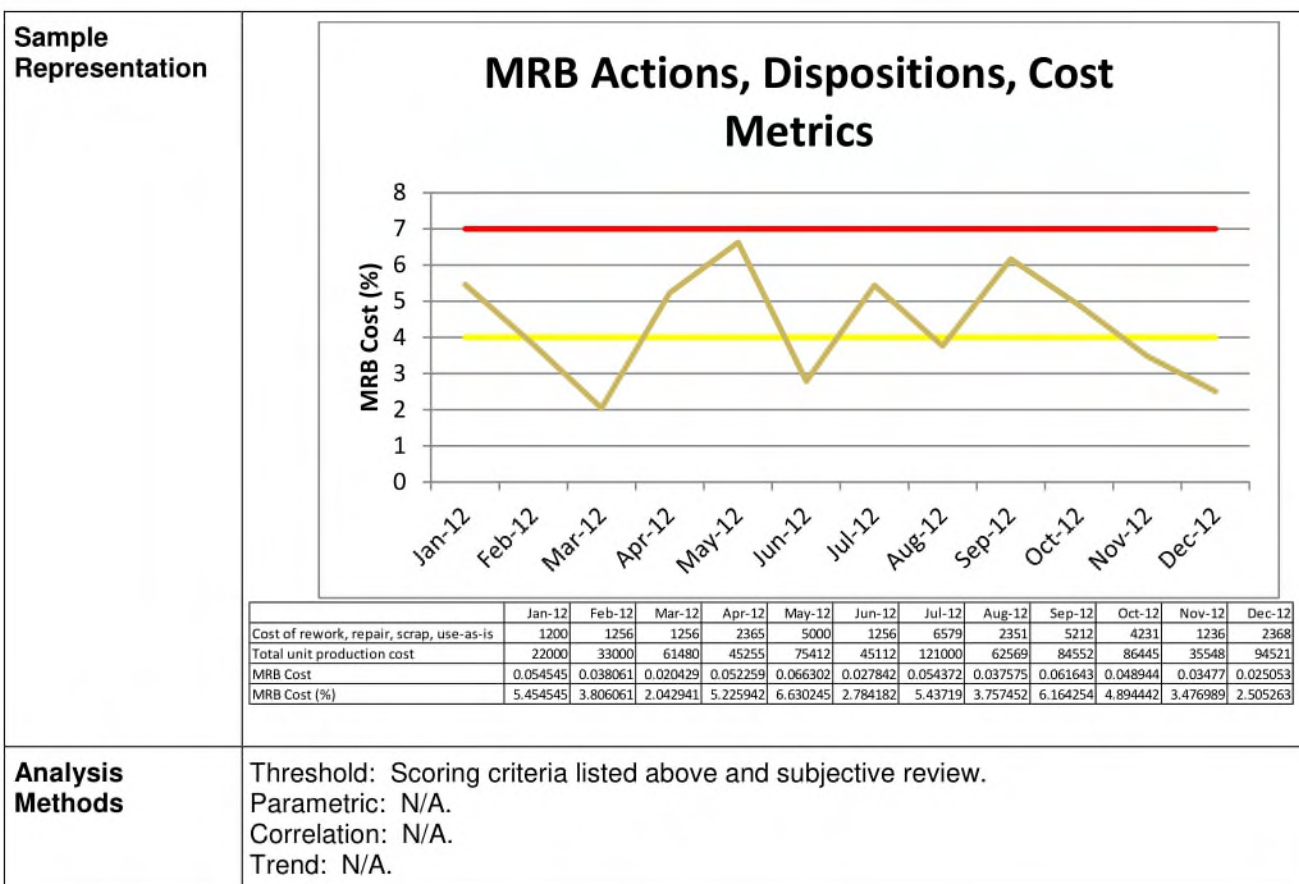
Sample
Representation**Critical vs Major Waivers Approved****Critical vs Major Deviations Approved**

	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Total count of critical waivers approved	0	0	0	1	0	0	2	1	0	0	1	0
Total count of major waivers approved	1	0	0	1	0	0	0	0	1	1	2	2
Total count of critical deviations approved	1	0	0	0	0	0	0	0	1	1	0	0
Total count of major deviations approved	2	0	0	2	0	0	2	1	2	2	3	2
Total count of critical waivers submitted to the MDA CCB for approval	0	1	1	0	2	2	2	1	1	1	2	2
Total count of critical deviations submitted to the MDA CCB for approval	1	2	1	1	3	1	1	1	1	1	1	1



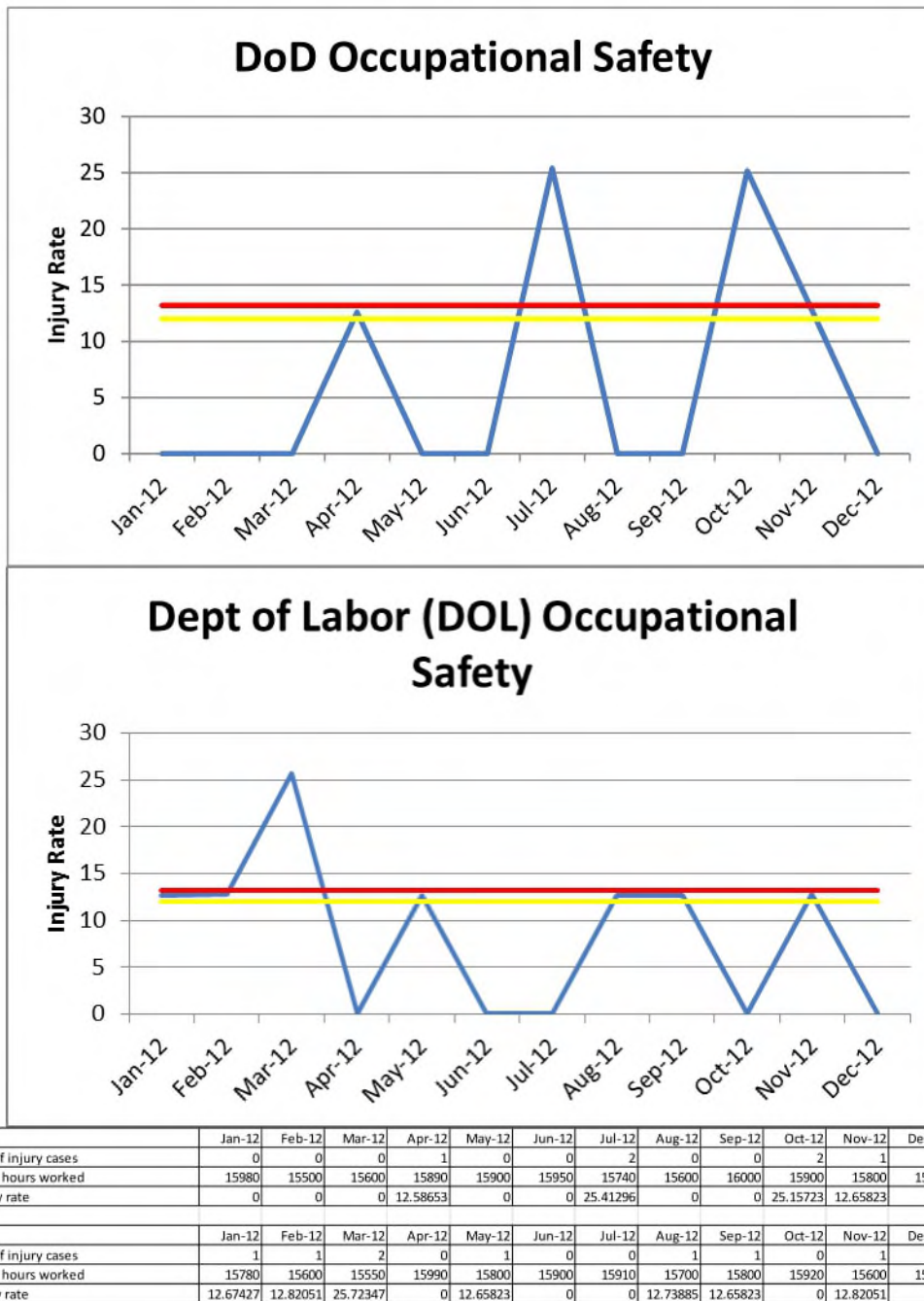
B.4.7.16 Material Review Board Actions, Dispositions, and Cost Metrics

Description	Material Review Board (MRB) actions, dispositions, and cost metrics is that effort associated with bringing contractors' items, products, or materials back into compliance once they are found to be incomplete or not in conformance.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Material Review Board actions, dispositions, and cost metrics is applicable to all MDA programs. Answers the questions: a. What percent of effort is utilized to correct or change products (intermediate or final) once they are found to be incomplete or not in conformance? b. How accurately was MRB Cost estimated?
Data Primitives Collected	Separately report MRB actions, dispositions, and cost metrics. Metrics include: a. Cost of rework, repair, scrap, and use-as-is as it relates to first pass yield per delivered product. b. Total unit production cost.
Aggregate Values Calculated	$MRB\ Cost\ Percentage = \frac{Cost\ of\ (rework + repair + scrap + use\ as\ is)}{Total\ unit\ production\ cost} \times 100$
Scoring Criteria	Cost of rework + repair + scrap + use-as-is as it relates to first pass yield per delivered product: GREEN: $1\% \leq MRB\ Cost \leq 4\%$ YELLOW: $4\% \leq MRB\ Cost \leq 7\%$ RED: $MRB\ Cost > 7\%$



B.4.7.17 Occupational Safety

Description	Missile Defense Agency (MDA) injury/fatality rate. These measures consist of injury and fatality rates for civilians and military personnel. MDA/QS has adopted and modified these criteria to include civilian work related injury rate, military assigned on-duty injury rate and military assigned off-duty injury rate.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	<p>Injury rates apply to MDA assigned civilians and contractors supervised by Government personnel in their work place. (Effective January 2005).</p> <p>Injury rates apply to MDA assigned military on-duty and off-duty.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> How do MDA Injury/Accident rates compare with Department of Defense (DOD) Injury/Accident Rates and Department of Labor (DOL) civilian lost time injury rate? How do MDA Injury/Accident rates compare with MDA previous years and cumulative years rates?
Data Primitives Collected	<ol style="list-style-type: none"> Number of injury cases. Total man hours worked.
Aggregate Values Calculated	The number of cases X 200,000 man hours divided by total man hours worked.
Scoring Criteria	<p>GREEN: Civilian and contractor injury rate < the DOL target rate, and Military injury rate < the DOD target rate</p> <p>YELLOW: Civilian or contractor injury rate \geq to the DOL target rate or less than 10% above DOL target rate, or Military injury rate \geq to the DOD target rate or less than 10% above DOD target rate</p> <p>RED: Civilian or contractor injury rate \geq the DOL target rate by 10%, or Military injury rate \geq the DOD target rate by 10%</p>

**Sample
Representation**

**Analysis
Methods**

Threshold: Scoring criteria listed above and subjective review.
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

B.4.7.18 System Safety Progress

Description	To gauge the progress of MDA Program Office/Program system safety programs.		
Critical Area	Adequacy, Quality, Safety, and Performance		
Application	<p>All MDA Program Offices and Programs.</p> <p>Answers the question:</p> <p>Are MDA Program Offices/Programs making progress with their system safety programs?</p>		
Data Primitives Collected	<p>Contractors will report the following values:</p> <ul style="list-style-type: none"> a. Difference in days between end of the period covered in current report and report date. b. Number of open hazards with current hazard risk indices in the High and Serious risk levels. c. Number of open hazards with expected final hazard risk indices in the High and Serious risk levels. 		
Aggregate Values Calculated	No computation required.		
Scoring Criteria	GREEN	Value "a" <30 And Value "b" =0 And Value "c" =0	
	YELLOW	(30≤Value "a" <60 or Value "b" >0) And Value "c" =0	
	RED	Value "a" ≥60 or Value "c" >0	

Sample Representation	Thresholds	Red	Yellow	Red	Green	Yellow	Red	Red	Green	Red	Red	Yellow	Red
		Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
	a. Difference in days between end of the period covered in current report and report date.	34	55	65	29	52	36	12	25	18	11	45	36
	b. Number of open hazards with current hazard risk indices in the High and Serious risk levels	5	4	0	0	6	4	0	0	2	0	1	2
	c. Number of open hazards with expected final hazard risk indices in the High and Serious risk levels	2	0	2	0	0	2	5	0	2	5	0	3
Analysis Methods	Threshold: Scoring criteria listed above and subjective review.												
	Parametric: N/A. Correlation: N/A. Trend: N/A.												

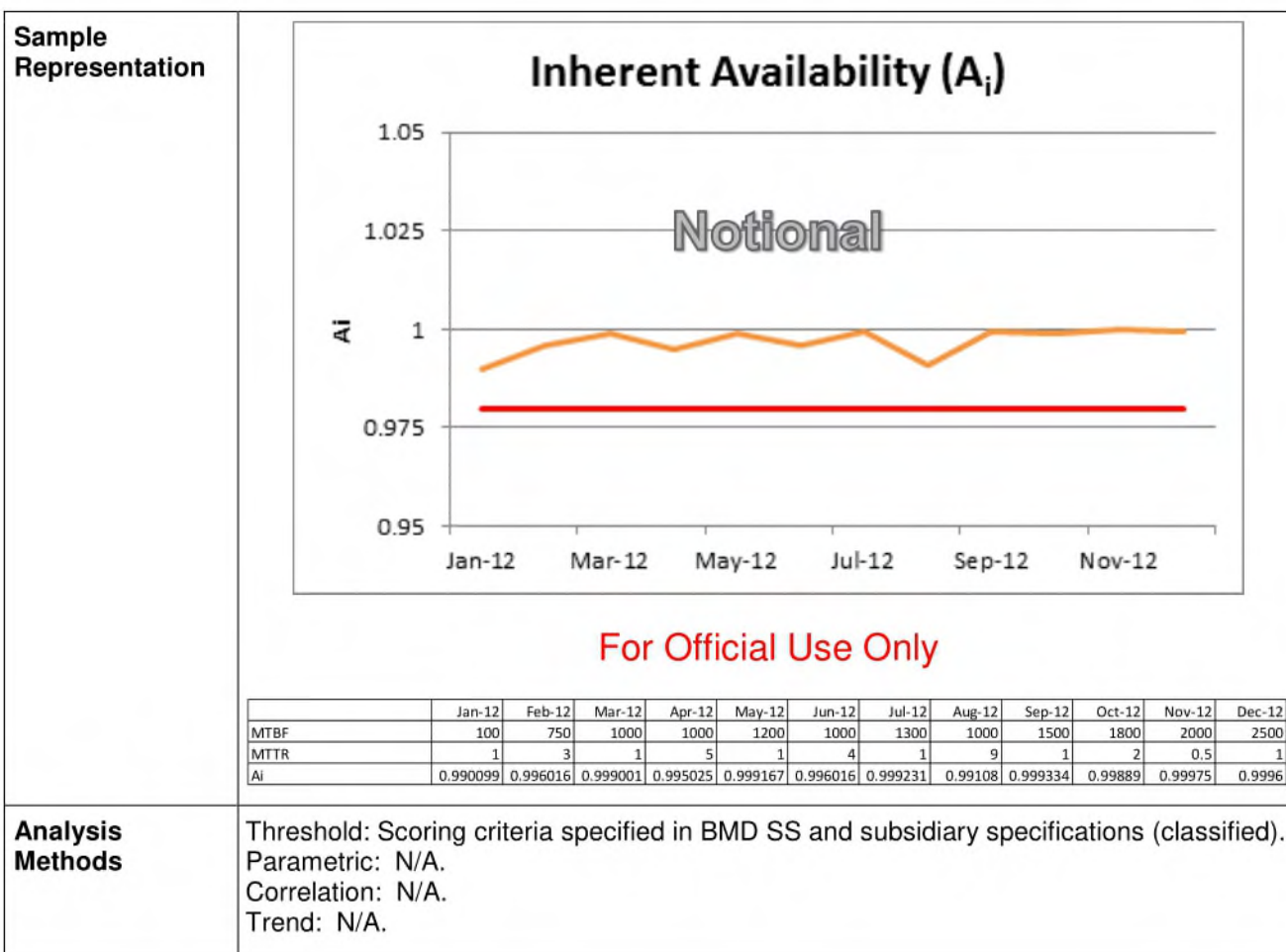
B.4.7.19 Software Safety Status

Description	To gauge the status of MDA Program Office/Program software safety activities.	
Critical Area	Adequacy, Quality, Safety, and Performance	
Application	All MDA Program Offices and Programs. Answers the question: To what extent have safety critical software requirements been identified, traced to code, and verified?	
Data Primitives Collected	Contractors shall provide the following values: a. Difference in days between end of the period covered in current report and report date. b. % of software requirements contained in current Software Requirements Specification (SRS) examined to identify safety critical requirements, to be reported upon release of SRS. c. % of safety critical software requirements for which code has been written. d. % of safety critical software requirements traced to code. e. % of safety critical software requirements traced to verification activities, to be reported upon release of verification plans. f. % of safety critical software requirements scheduled for verification. g. % of safety critical software requirements verified.	
Aggregate Values Calculated	No computation required.	
Scoring Criteria	GREEN	Value "a" ≤60 And Value "b" = 100% And Value "c" = Value "d" And Value "e" = 100% And Value "f" = "Value "g"
	YELLOW	60 < Value "a" ≤ 90 Or 0.8 * Value "c" ≤ Value "d" < Value "c" Or 0.8 * Value "f" ≤ Value "g" < Value "f"
	RED	Value "a" > 90 Or Value "b" < 100% Or Value "d" < 0.8 * Value "c" Or Value "e" < 100% Or Value "g" < 0.8 * Value "f"

Sample Representation		Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
	a. Difference (in days) between end of the period covered in current report and report date	55	52	45	62	45	80	60	75	45	95	88	45
	b. % of software requirements contained in current software requirements specification (SRS) examined to identify safety-critical requirements, to be reported upon release of SRS	100	100	92	100	95	85	100	62	77	88	92	96
	c. % of safety-critical software requirements for which code has been written	45	45	11	75	45	56	62	88	0	44	0	45
	d. % of safety-critical software requirements traced to code	45	95	0	75	55	47	62	48	0	45	55	45
	e. % of safety-critical software requirements traced to verification activities, to be reported upon release of verification plans.	100	94	92	97	100	78	100	78	100	88	94	99
	f. % of safety-critical software requirements scheduled for verification	45	7	75	77	15	45	45	0	4	5	78	45
	g. % of safety-critical software requirements verified	45	25	55	14	86	45	45	0	45	23	45	45
	Thresholds	Green			Yellow		Yellow		Yellow			Yellow	
			Red	Red	Red	Red	Red		Red	Red	Red	Red	Red
Analysis Methods	Threshold: Scoring criteria listed above and subjective review. Parametric: N/A. Correlation: N/A. Trend: N/A.												

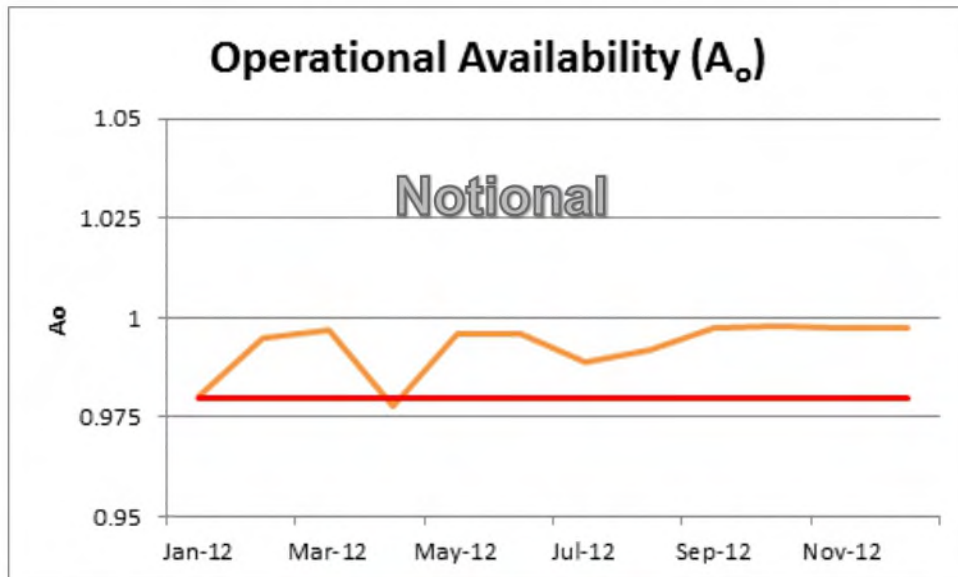
B.4.7.20 Inherent Availability

Description	Inherent Availability (A_i) is defined as Availability of a system with respect only to operating time and corrective maintenance. Inherent Availability (A_i) ignores standby and delay times associated with preventive maintenance as well as administrative and logistics down time.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Inherent Availability (A_i) is applicable to all BMD Elements, and to the BMDS. Answers the question: Does the reported Inherent Availability (A_i) value meet or exceed the value specified in the BMD System Specification (BMD SS) or subsidiary specifications?
Data Primitives Collected	Separately report element and component values quarterly for the current period and cumulative: Inherent Availability (A_i) MTBCF is the Mean Time Between Critical Failures Mean Time to Repair (MTTR - see B.4.7.22)
Aggregate Values Calculated	$A_i = \frac{MTBCF}{MTBCF + MTTR}$
Scoring Criteria	Inherent Availability (A_i) threshold values are contained in the classified BMD SS document and subsidiary specifications.



B.4.7.21 Operational Availability

Description	Operational Availability (A_O) is the probability that the system will be ready to perform its specified function, in its specified and intended operational environment, when called for at a random point in time.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Operational Availability (A_O) is applicable to all BMD Elements, and to the BMDS. Answers the question: Does the reported Operational Availability (A_O) value meet or exceed the value specified in the BMD SS or subsidiary specifications?
Data Primitives Collected	Separately report element and component values quarterly for the current period and cumulative: Operational Availability (A_O) Mean Time to Repair (MTTR - see B.4.7.22) Mean Time Between Critical Failures (MTBCF - see B.4.7.24 and B.4.7.25) Mean Logistics Delay Time (MLDT - see B.4.7.26) Mean Schedule Maintenance Downtime (MSMDT) NOTE: In all cases, "Critical Failure" means any fault, failure, or malfunction that results in the loss of any mission essential function. Critical failures do not always occur during mission time; they merely must or could cause mission impact. Hardware and software failures, operator errors, and errors in technical orders that cause such a loss are normally counted as critical failures.
Aggregate Values Calculated	$A_O = \frac{MTBCF}{MTBCF + MTTR + MSMDT + MLDT}$
Scoring Criteria	Operational Availability (A_O) threshold values are contained in the classified BMD SS document and subsidiary specifications.

Sample Representation

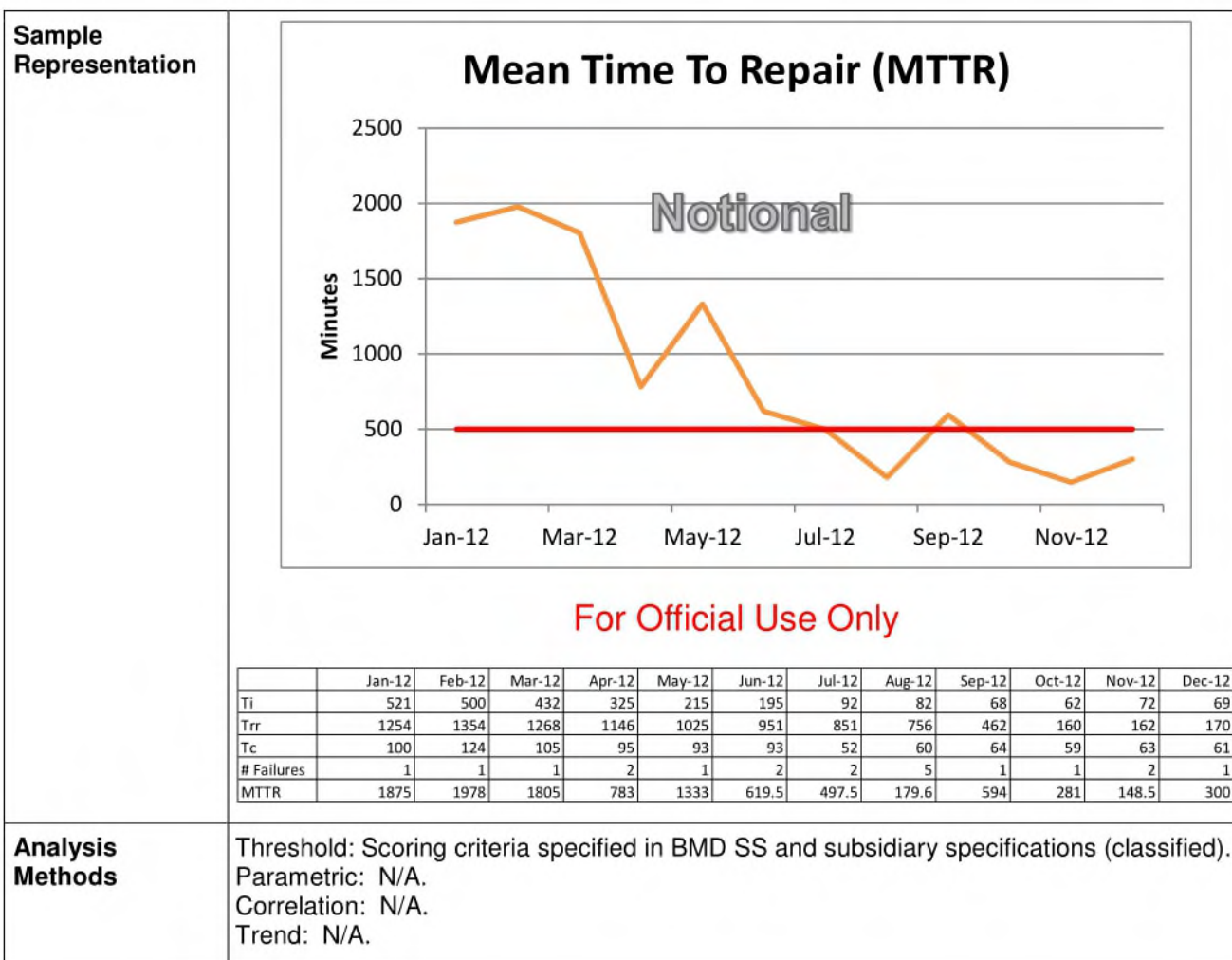
	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
MTBCF	100	750	1000	1000	1200	1000	1300	1000	1500	1800	2000	2500
MTTR	1	2	1	20	1	1	10	1	2	1	2	3
MSMDT	0	1	1	1	3	1	1	1	1	2	1	2
MLDT	1	1	1	2	1	2	4	6	1	1	2	1
A_o	0.980392	0.994695	0.997009	0.977517	0.995851	0.996016	0.988593	0.992063	0.99734	0.997783	0.997506	0.997606

Analysis Methods

Threshold: Scoring criteria specified in BMD SS and subsidiary specifications (classified).
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

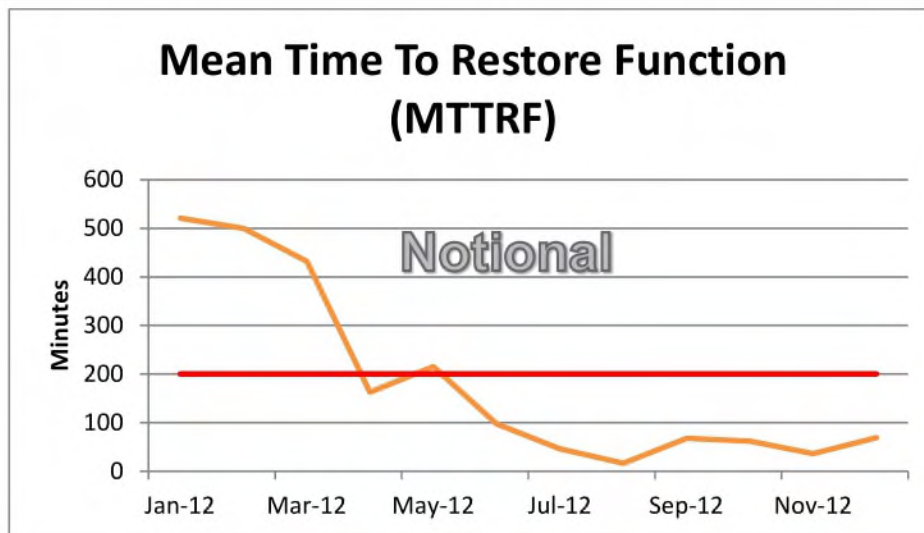
B.4.7.22 Mean Time To Repair

Description	Mean Time To Repair (MTTR) is the average time required to bring the system from a failed state to an operable state. Assumes maintenance personnel and spares are on hand. Typically includes isolation, remove and replacement of failed item(s), and checkout.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	MTTR is applicable to all BMD Elements. Answers the questions: a. Does the reported MTTR value meet or exceed the value specified in the BMD SS? b. What impact does the reported MTTR value have on BMD Element and major Element subsystem Operational Availability (A_O)?
Data Primitives Collected	Separately report element and component values quarterly for the current period and cumulative: MTTR T_i = Fault Isolation Time (minutes) for each occurrence T_{rr} = Remove and Replace, Repair, Restore Time for each occurrence T_c = Checkout Time for each occurrence $\# Failures$ = Total number of critical failures NOTE: In all cases, "Critical Failure" means any fault, failure, or malfunction that results in the loss of any mission essential function. Critical failures do not always occur during mission time; they merely must or could cause mission impact. Hardware and software failures, operator errors, and errors in technical orders that cause such a loss are normally counted as critical failures.
Aggregate Values Calculated	$MTTR = \frac{\sum (T_i + T_{rr} + T_c)}{\# Failures}$
Scoring Criteria	MTTR threshold values are contained in the classified BMD SS document and subsidiary specifications.



B.4.7.23 Mean Time To Restore Function

Description	Mean Time To Restore Function (MTTRF) is the average time required, as the result of critical failure, to restore a system to full operating status. It includes administrative and logistics delay times associated with restoring function following a critical failure.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	MTTRF is applicable to all BMD Elements. Answers the questions: a. Does the reported MTTRF value meet or exceed the value specified in the BMD SS or subsidiary specifications? b. What impact does the reported MTTRF value have on BMDS and BMD Element maintainability?
Data Primitives Collected	Separately report element and component values quarterly for the current period and cumulative: MTTRF Total Critical Restore Time = Total time for fault isolation, remove, replace, admin delay, logistics delay, repair, restore, and checkout times associated with restoring function following a critical failure. # <i>Failures</i> = Total number of critical failures NOTE: In all cases, "Critical Failure" means any fault, failure, or malfunction that results in the loss of any mission essential function. Critical failures do not always occur during mission time; they merely must or could cause mission impact. Hardware and software failures, operator errors, and errors in technical orders that cause such a loss are normally counted as critical failures.
Aggregate Values Calculated	$\text{MTTRF} = \frac{\text{Total Critical Restore Time}}{\text{Total Number of Critical Failures}}$
Scoring Criteria	MTTRF threshold values are contained in the classified BMD SS document and subsidiary specifications.

Sample Representation

For Official Use Only

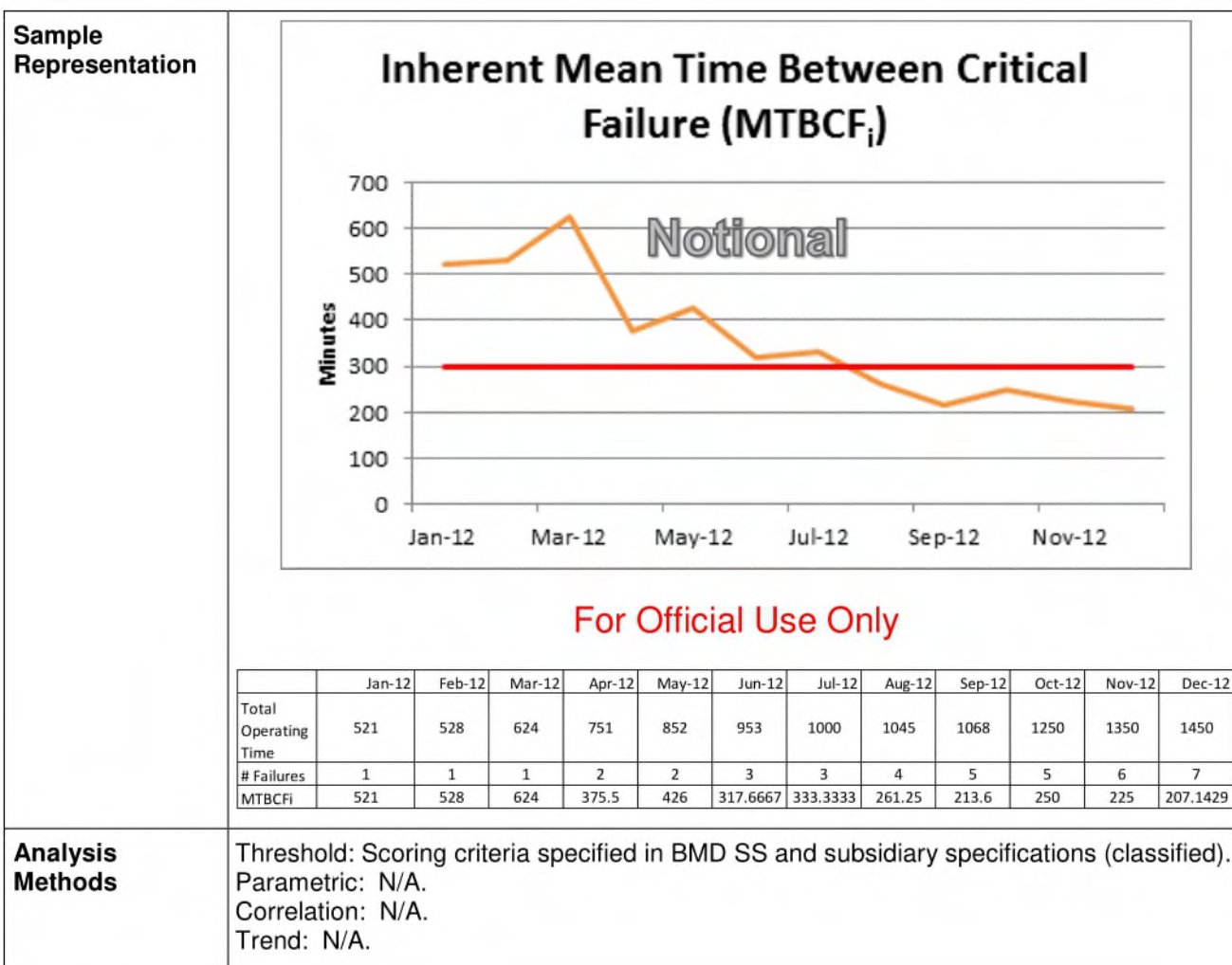
	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Total Critical Restore Time	521	500	432	325	215	195	92	82	68	62	72	69
Total Number of Critical Failures	1	1	1	2	1	2	2	5	1	1	2	1
MTTRF	521	500	432	162.5	215	97.5	46	16.4	68	62	36	69

Analysis Methods

Threshold: Scoring criteria specified in BMD SS and subsidiary specifications (classified).
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

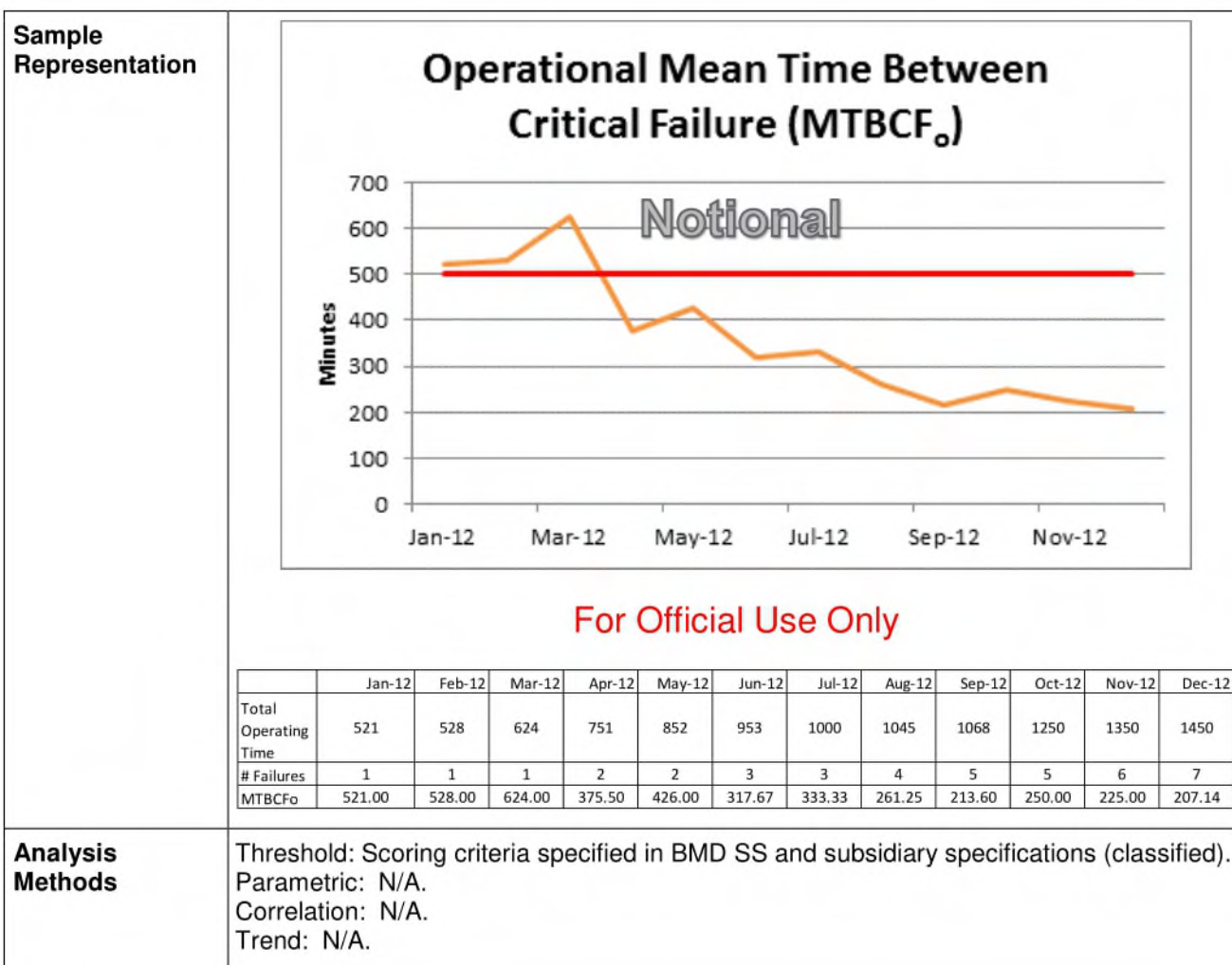
B.4.7.24 Inherent Mean Time Between Critical Failure

Description	Inherent Mean Time Between Critical Failure (MTBCF _i) is the average time between failures that cause a loss of system function defined as “critical” by the subsystem, or mission essential by the warfighter.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	MTBCF _i is applicable to all BMD Elements and used to calculate system Availability. Answers the questions: a. Does the reported MTBCF _i value meet or exceed the value specified in the BMD SS? b. What impact does the reported MTBCF _i value have on BMD Element Availability?
Data Primitives Collected	Separately report hardware and software element and component values quarterly for the current period and cumulative: At the BMD Element level, MTBCF _i is calculated using inherent critical failures due to the system design attributed to hardware, hardware BIT, software, software BIT, and firmware. This inherent statistic, while collected in various environments, will be compared with the BMD SS threshold and goal values, not for verification purposes, but in the context of progress made toward design goals. MTBCF _i T = Total Operating Time $\# \text{ Failures}$ = Total Number of combined hardware and software Mission Critical Failures NOTE: In all cases, “Critical Failure” means any fault, failure, or malfunction that results in the loss of any mission essential function. Critical failures do not always occur during mission time; they merely must or could cause mission impact. Hardware and software failures, operator errors, and errors in technical orders that cause such a loss are normally counted as critical failures.
Aggregate Values Calculated	$\text{MTBCF}_i = \frac{T}{\# \text{ Failures}}$
Scoring Criteria	MTBCF _i threshold values are contained in the classified BMD SS document and subsidiary specifications.



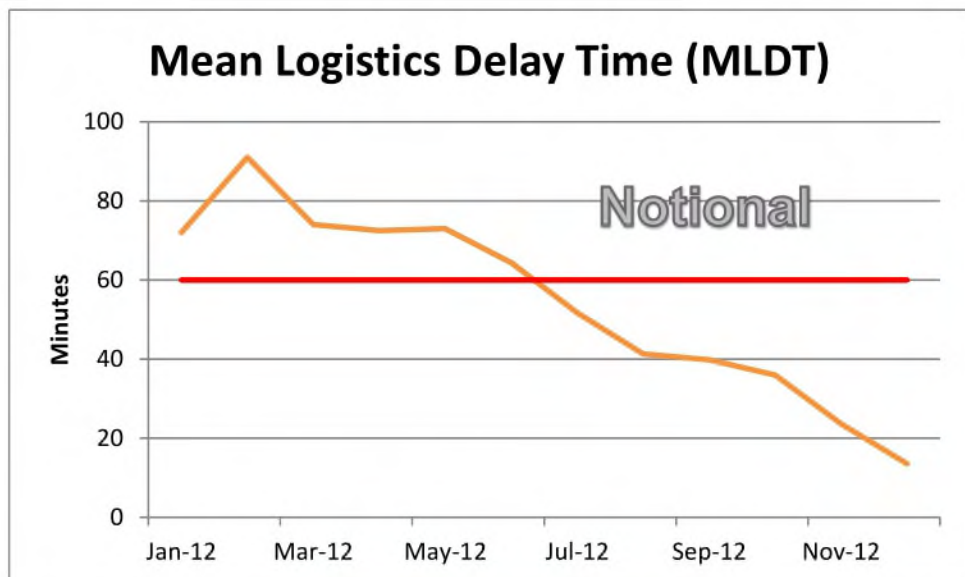
B.4.7.25 Operational Mean Time Between Critical Failure

Description	Operational Mean Time Between Critical Failure (MTBCF _o) is the average time between failures that cause a loss of system function defined as "critical" by the subsystem, or mission essential by the warfighter.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	MTBCF _o is applicable to all BMD Elements and used to calculate system Operational Availability (A _o). Answers the question: What impact does the reported MTBCF _o value have on BMD Element Availability (A _o)?
Data Primitives Collected	Separately report BMD Element and major Element Subsystems values quarterly for the current period and cumulative: MTBCF _o <i>T</i> = Total Operating Time <i># Failures</i> = Total Number of Mission Critical Failures NOTE: In all cases, "Critical Failure" means any fault, failure, or malfunction that results in the loss of any mission essential function. Critical failures do not always occur during mission time; they merely must or could cause mission impact. Hardware and software failures, operator errors, and errors in technical orders that cause such a loss are normally counted as critical failures.
Aggregate Values Calculated	$MTBCF_o = \frac{T}{\# Failures}$
Scoring Criteria	MTBCF _o threshold values are contained in the classified BMD SS document and subsidiary specifications.



B.4.7.26 Mean Logistics Delay Time

Description	Mean Logistics Delay Time (MLDT) is the average administrative and logistics delay time for critical failures. The MLDT includes delay time for spares, support equipment, personnel, facilities, transportation, and Administrative Delay Time (ADT).
Critical Area	Adequacy, Quality, Safety, and Performance
Application	<p>MLDT is applicable to all BMD Elements used to monitor the effectiveness of BMD Element and major Element Subsystems logistics infrastructures and to calculate BMD Element and major Element Subsystems Availability (A_0).</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Does the reported MLDT value meet or exceed the value specified in the BMD SS? What impact does the reported MLDT value have on BMD Element and major Element Subsystem Availability (A_0)?
Data Primitives Collected	<p>Separately report BMD Element and major Element Subsystem values quarterly for the current period and cumulative:</p> <p>Mean Logistics Delay Time (MLDT)</p> <p>Dts = Delay time attributable to waiting for spare parts</p> <p>Dte = Delay time attributable to waiting for support and test equipment</p> <p>Dtp = Delay time attributable to waiting for personnel</p> <p>Dtf = Delay time attributable to waiting for facilities</p> <p>Dtt = Delay time attributable to transportation</p> <p>ADT = Administrative Delay Time. The ADT includes, for example, requisition processing time, or procurement lead time. Care must be exercised to avoid "double counting" ADT and one or more of the other listed delay times.</p> <p>$\# Failures$ = Total Number of Critical Failures</p> <p>NOTE: In all cases, "Critical Failure" means any fault, failure, or malfunction that results in the loss of any mission essential function. Critical failures do not always occur during mission time; they merely must or could cause mission impact. Hardware and software failures, operator errors, and errors in technical orders that cause such a loss are normally counted as critical failures.</p>
Aggregate Values Calculated	$MLDT = \frac{\sum (Dts + Dte + Dtp + Dtf + Dtt + ADT)}{\# Failures}$
Scoring Criteria	MLDT threshold values will be contained in the classified BMD SS document and subsidiary specifications.

Sample Representation

For Official Use Only

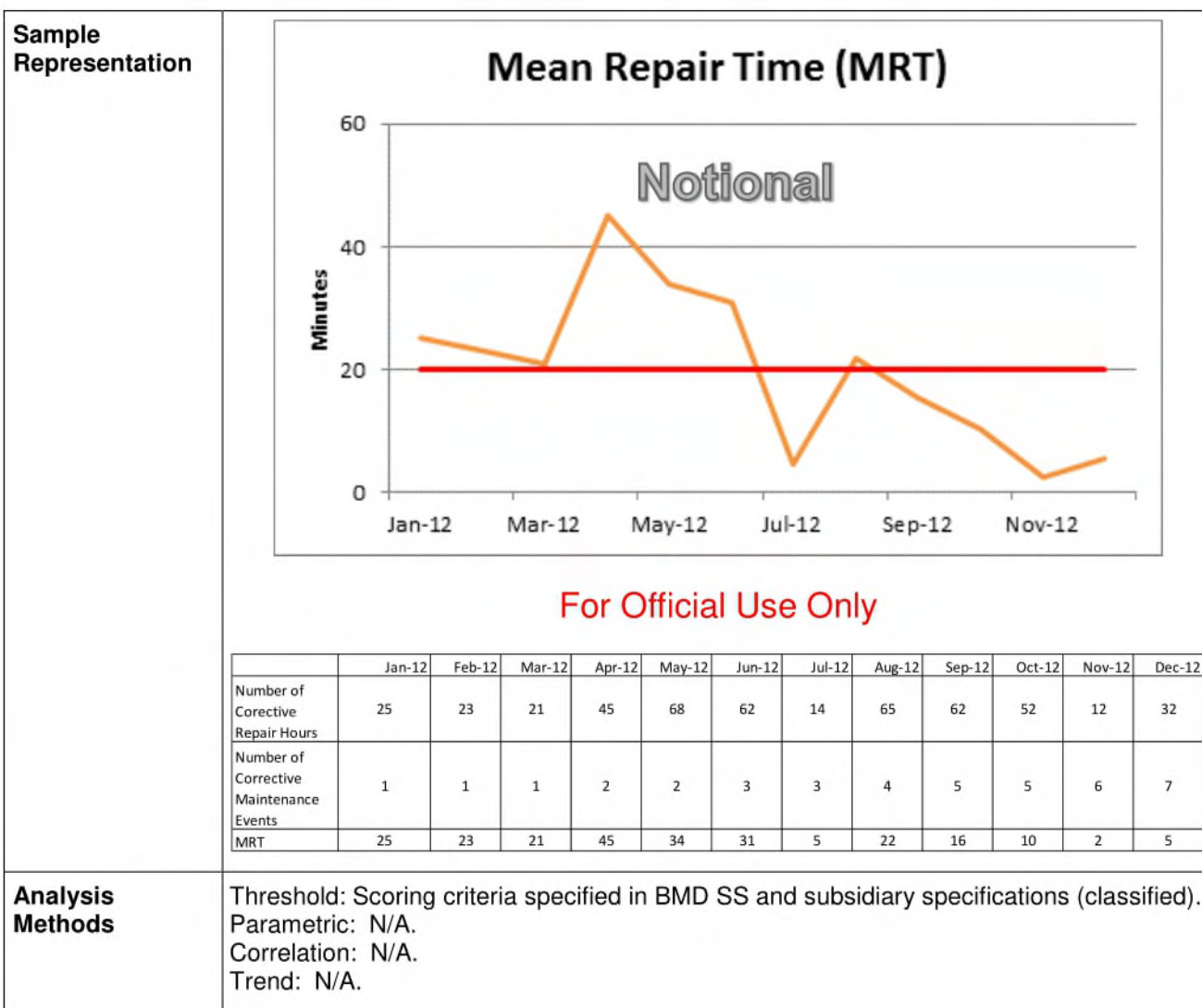
	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Dts	25	23	21	45	68	62	14	65	62	52	12	32
Dte	12	32	20	23	12	45	62	12	32	45	23	21
Dtp	0	0	21	23	0	21	25	23	0	21	23	0
Dtf	0	32	0	0	0	0	0	23	0	0	21	0
Dtt	12	4	12	54	45	65	54	42	53	62	51	42
ADT	23	0	0	0	21	0	0	0	52	0	12	0
# Failures	1	1	1	2	2	3	3	4	5	5	6	7
MLDT	72	91	74	73	73	64	52	41	40	36	24	14

Analysis Methods

Threshold: Scoring criteria specified in BMD SS and subsidiary specifications (classified).
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

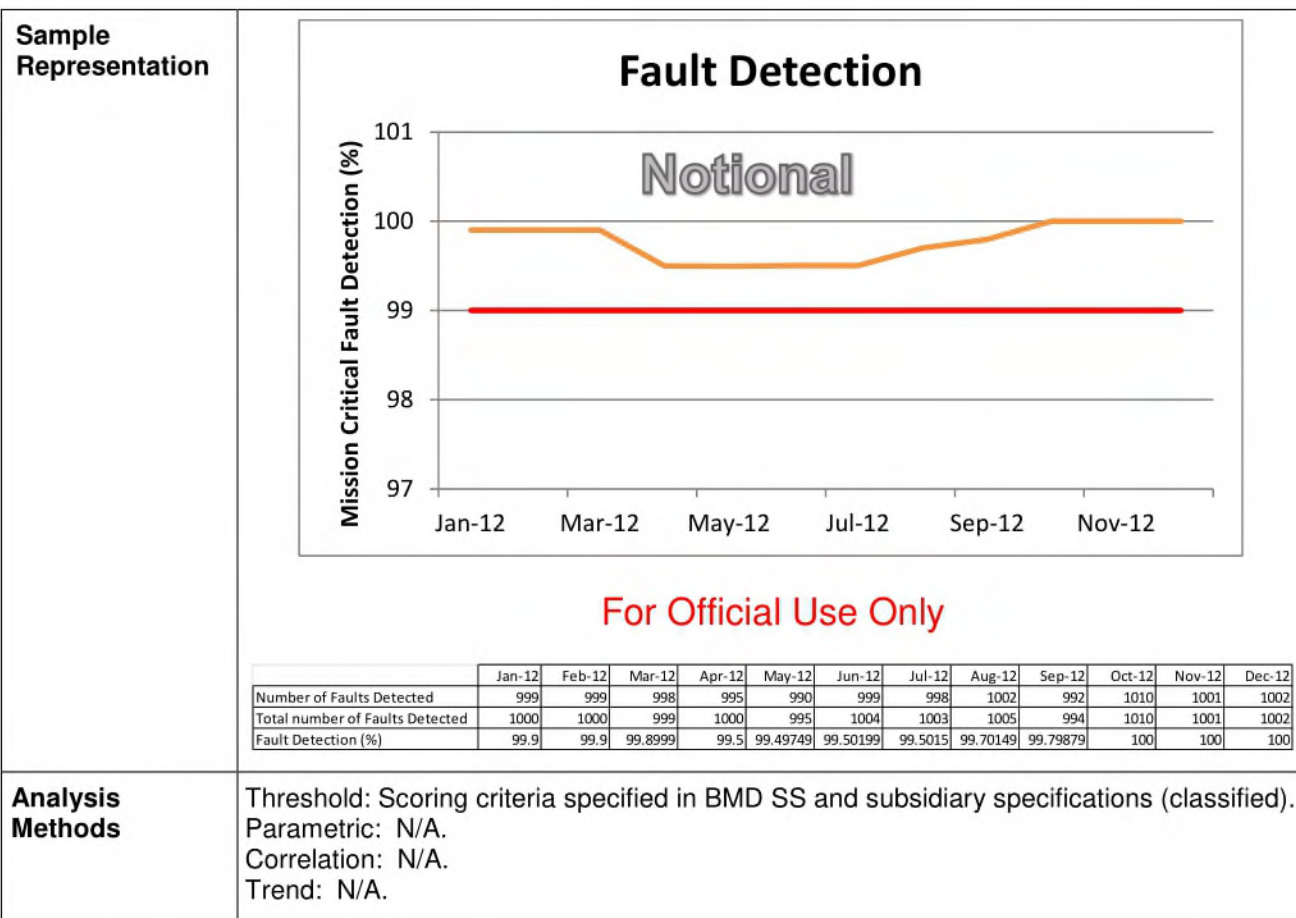
B.4.7.27 Mean Repair Time

Description	Mean Repair Time (MRT) is the average on-equipment, off-equipment or both corrective maintenance times. It includes all maintenance actions needed to correct a malfunction, including preparing for test, troubleshooting, removing and replacing components, repairing, adjusting, re-assembly, alignment, adjustment, and checkout. The MRT does not include maintenance, supply, or administrative delays. Note: MRT differs from the contractual term Mean Time To Repair (MTTR) in that it measures activities that occur in the operational environment.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	<p>MRT is applicable to all BMD Elements and used to monitor the effectiveness of BMD Element and major Element Subsystems logistics infrastructures to correct a malfunction, including preparing for test, troubleshooting, removing and replacing components, repairing, adjusting, reassembly, alignment, adjustment, and checkout.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Does the reported MRT value meet or exceed the value specified in the BMD SS or subsidiary specifications? What impact does the reported MRT value have on BMD Element and major Element Subsystems Maintainability (i.e., MTTR)?
Data Primitives Collected	<p>Separately report BMD Elements and major subsystems values quarterly for the current period and cumulative:</p> <p>MRT <i>Failures</i> = Total Number of Critical Failures Number of Corrective Repair Hours Number of Corrective Maintenance Events</p> <p>NOTE: In all cases, "Critical Failure" means any fault, failure, or malfunction that results in the loss of any mission essential function. Critical failures do not always occur during mission time; they merely must or could cause mission impact. Hardware and software failures, operator errors, and errors in technical orders that cause such a loss are normally counted as critical failures.</p>
Aggregate Values Calculated	$MRT = \frac{\text{Number of Corrective Repair Hours}}{\text{Number of Corrective Maintenance Events}}$
Scoring Criteria	MRT threshold values will be contained in the classified BMD SS document and subsidiary specifications.



B.4.7.28 Fault Detection

Description	Fault Detection is a measure of the number of faults correctly detected by the system to the total number of faults experienced by the system, typically expressed as a percent
Critical Area	Adequacy, Quality, Safety, and Performance
Application	<p>Fault Detection is applicable to all BMD Elements, and to the BMDS.</p> <p>Answers the question:</p> <p>Does the reported Fault Detection value meet or exceed the value specified in the BMD System Specification (BMD SS) or subsidiary specifications?</p>
Data Primitives Collected	<p>Separately report element and component values quarterly for the current period and cumulative:</p> <p>Percent Fault Detected</p> <ul style="list-style-type: none"> a. Number of Faults Detected b. Total Number of Faults
Aggregate Values Calculated	$\text{Fault Detection Percentage} = \frac{\# \text{Faults Detected}}{\text{Total Number of Faults}} \times 100$
Scoring Criteria	Fault Detection threshold values are contained in the classified BMD SS document and subsidiary specifications.

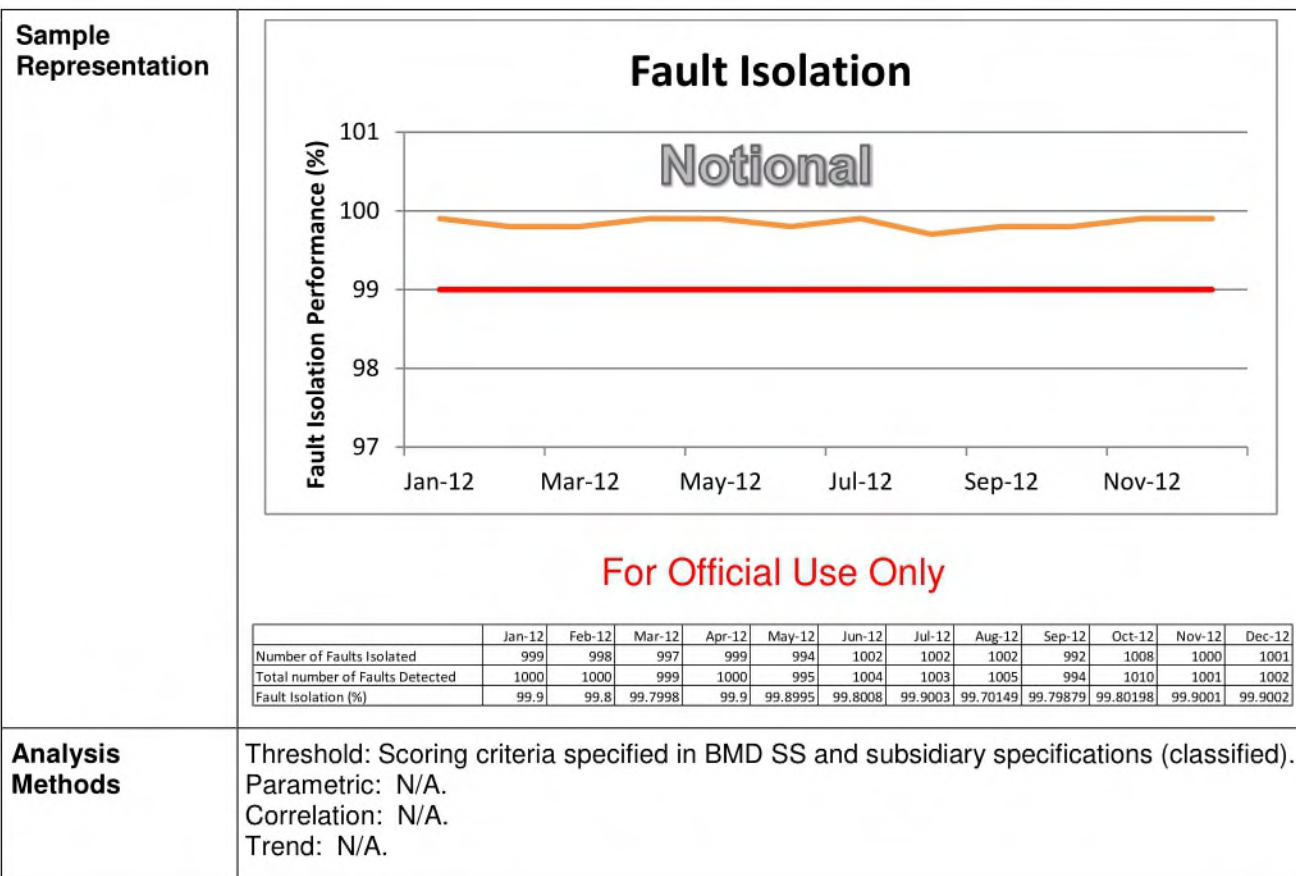


Analysis Methods

Threshold: Scoring criteria specified in BMD SS and subsidiary specifications (classified).
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

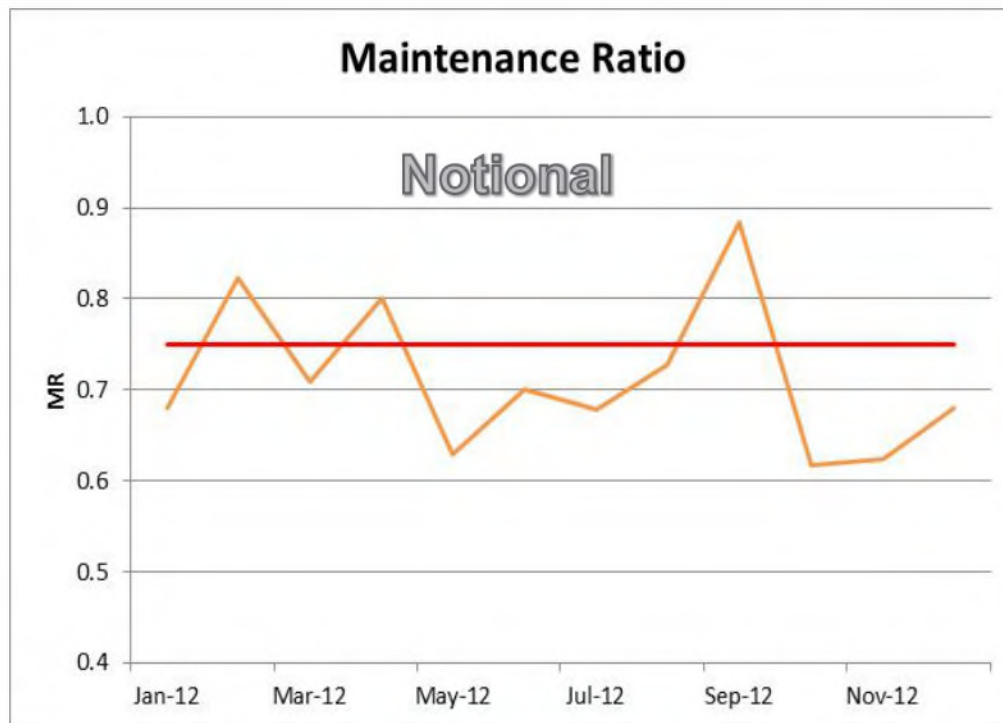
B.4.7.29 Fault Isolation

Description	Fault Isolation is a measure of the number of faults correctly isolated by the system to a specified level or assembly to the total number of faults detected by the system, typically expressed as a percent.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	<p>Fault Isolation is applicable to all BMD Elements, and to the BMDS.</p> <p>Answers the question:</p> <p>Does the reported Fault Isolation value meet or exceed the value specified in the BMD System Specification (BMD SS) or subsidiary specifications?</p>
Data Primitives Collected	<p>Separately report element and component values quarterly for the current period and cumulative:</p> <p>Percent Fault Isolation</p> <ol style="list-style-type: none"> Number of Faults Isolated Total Number of Faults Detected
Aggregate Values Calculated	$\text{Fault Isolation Percentage} = \frac{\# \text{Faults Isolated}}{\# \text{Faults Detected}} \times 100$
Scoring Criteria	Fault Isolation threshold values are contained in the classified BMD SS document and subsidiary specifications.



B.4.7.30 Maintenance Ratio

Description	Maintenance Ratio is measure of the total maintenance labor burden required to maintain an item. It is expressed as the cumulative number of labor hours of maintenance expended during a given period divided by the cumulative number of operating hours.
Critical Area	Adequacy, Quality, Safety, and Performance
Application	Maintenance Ratio is applicable to all BMD Elements, and to the BMDS. Answers the question: Does the reported Maintenance Ratio value meet or exceed the value specified in the BMD System Specification (BMD SS) or subsidiary specifications?
Data Primitives Collected	Separately report element and component values quarterly for the current period and cumulative: Maintenance Ratio # of Maintainers Corrective Maintenance (CM) Time Preventive Maintenance (PM) Time Operating Time Maintenance Man Hours (MMH) is calculated by multiplying maintenance time by number of maintainers.
Aggregate Values Calculated	$\text{Maintenance Ratio} = \frac{\text{Total MMH for CM} + \text{Total MMH for PM}}{\text{Total Operating Time}}$
Scoring Criteria	Maintenance Ratio threshold values are contained in the classified BMD SS document and subsidiary specifications and/or the User's Capabilities Production Document.

**Sample
Representation****For Official Use Only**

	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12
Maintenance Ratio (MR)	0.68	0.822222	0.709091	0.8	0.628571	0.7	0.678261	0.727273	0.884211	0.616667	0.624	0.68
# of Maintainers	2	2	2	2	2	2	2	2	2	2	2	2
Corrective Maintenance (CM) Time	70	85	95	90	65	75	95	100	110	85	95	70
Preventive Maintenance (PM) Time	100	100	100	100	100	100	100	100	100	100	100	100
Operating Time	500	450	550	475	525	500	575	550	475	600	625	500
Maintenance Man Hours (MMH) for CM	140	170	190	180	130	150	190	200	220	170	190	140
Maintenance Man Hours (MMH) for PM	200	200	200	200	200	200	200	200	200	200	200	200

**Analysis
Methods**

Threshold: Scoring criteria specified in BMD SS and subsidiary specifications (classified).
 Parametric: N/A.
 Correlation: N/A.
 Trend: N/A.

B.4.8 Software Development Environment

Software Development Environment addresses the software productivity, languages selected, adoption of software development best practices, exhibited elements of reuse, efficiency of the software development team, and other factors that describe the environment of the software development. The indicators for Software Development Environment are:

B.4.8.1 Software Productivity.

B.4.8.2 Software Requirements Ambiguity.

B.4.8.3 Software Requirements Incompleteness.

B.4.8.4 Software Reuse Profile.

B.4.8.5 Programming Languages Profile.

B.4.8.6 Resource Utilization.

B.4.8.7 Cyclomatic Complexity.

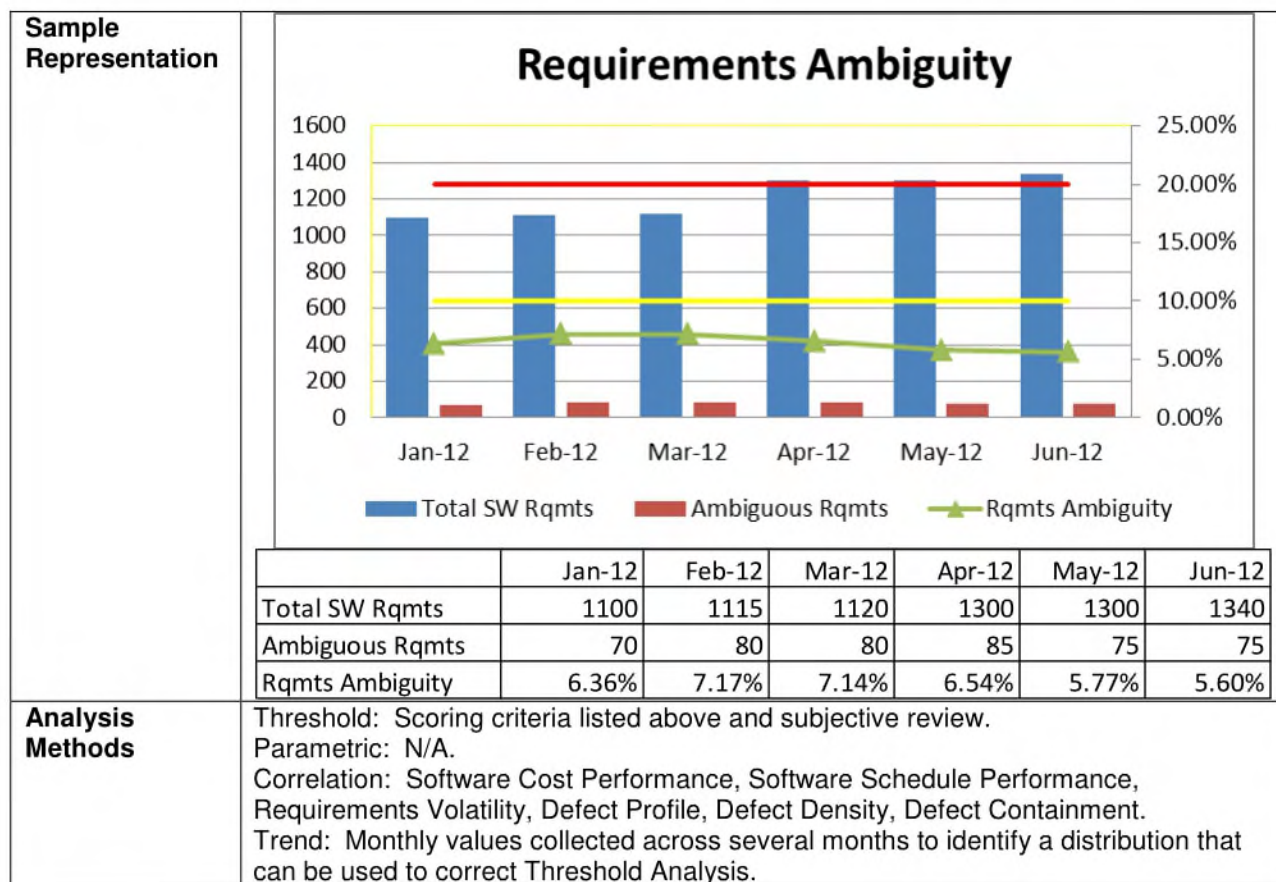
B.4.8.1 Software Productivity

Description	The Software Productivity indicator identifies the development organization's overall ability to produce software products across the life cycle. It identifies the work products in terms of ESLOC and the time spent developing them. Software Productivity is an indicator of ability to complete products as contracted and a predictor of future product development.
Critical Area	Software Development Environment
Application	Applicable to all MDA software development programs. Collected by software build and major component at software release. Answers the question: How productive is the contractor in developing software products?
Data Primitives Collected	<ul style="list-style-type: none"> a. Delivered New SLOC. b. Delivered Modified SLOC. c. Delivered Reuse SLOC. d. Delivered Auto-Generated SLOC. e. Software Development Activity Hours (hours spent on software development and supporting activities).
Aggregate Values Calculated	<ul style="list-style-type: none"> a. $ESLOC = New + (0.5) \times Modified + (0.05) \times Reuse + (0.3) \times Auto-Generated$ b. $Software\ Productivity = Software\ Development\ Activity\ Hours / ESLOC$
Scoring Criteria	There is no scoring criteria for Software Productivity

Sample Representation	<div><h3>Software Productivity</h3><table><thead><tr><th></th><th>Build 1.1</th><th>Build 1.2</th><th>Build 1.3.x</th></tr></thead><tbody><tr><td>Delivered New</td><td>25000</td><td>10000</td><td>20000</td></tr><tr><td>Delivered Modified</td><td>65000</td><td>5000</td><td>15000</td></tr><tr><td>Delivered Reuse</td><td>125000</td><td>250000</td><td>270000</td></tr><tr><td>Delivered Auto</td><td>35000</td><td>5000</td><td>10000</td></tr><tr><td>Total SW Hours</td><td>73498</td><td>35000</td><td>49492</td></tr><tr><td>Equivalent SLOC</td><td>74250</td><td>26500</td><td>44000</td></tr><tr><td>SW Productivity</td><td>0.99</td><td>1.32</td><td>1.12</td></tr></tbody></table></div>		Build 1.1	Build 1.2	Build 1.3.x	Delivered New	25000	10000	20000	Delivered Modified	65000	5000	15000	Delivered Reuse	125000	250000	270000	Delivered Auto	35000	5000	10000	Total SW Hours	73498	35000	49492	Equivalent SLOC	74250	26500	44000	SW Productivity	0.99	1.32	1.12
		Build 1.1	Build 1.2	Build 1.3.x																													
Delivered New	25000	10000	20000																														
Delivered Modified	65000	5000	15000																														
Delivered Reuse	125000	250000	270000																														
Delivered Auto	35000	5000	10000																														
Total SW Hours	73498	35000	49492																														
Equivalent SLOC	74250	26500	44000																														
SW Productivity	0.99	1.32	1.12																														
Analysis Methods	<p>Threshold: Subjective review and comparison to proposed contract productivity levels.</p> <p>Parametric: Use of software productivity prediction models (i.e., COCOMO II, SEER For Software) to validate dataset.</p> <p>Correlation: Software Cost Performance, Software Schedule Performance, Software Staffing, Software Staffing Profile, Requirements Volatility, Defect Profile, Software Size Estimate.</p> <p>Trend: Values collected across several components and builds to set a trend in productivity for software development by contractor and application type.</p>																																

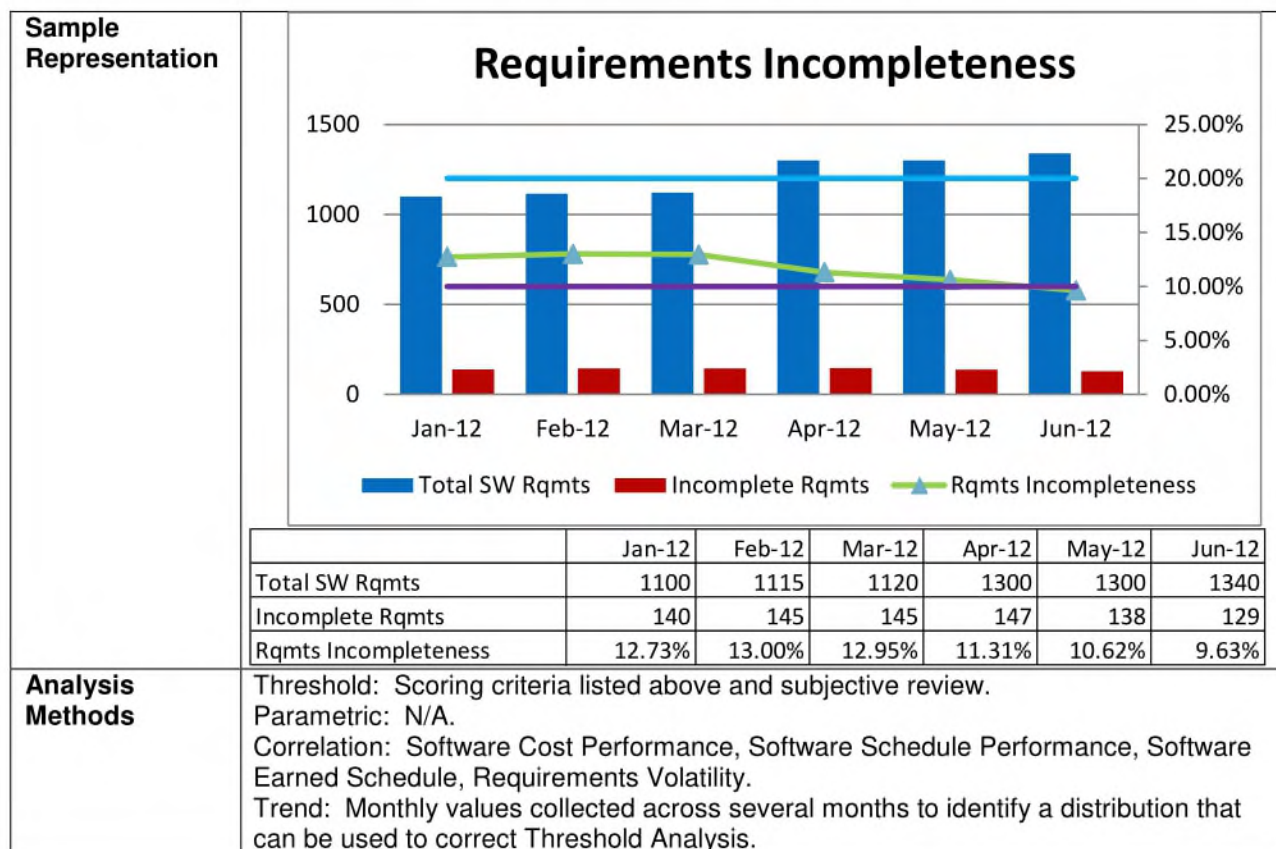
B.4.8.2 Software Requirements Ambiguity

Description	<p>The Software Requirements Ambiguity indicator identifies the level of uncertainty in the wording of the software requirements. Requirements ambiguity can lead to defects in design and code and subsequently, unplanned rework. The ambiguous phrases for requirements are listed below:</p> <p>“adequate”, “as acceptable”, “as appropriate”, “as a minimum”, “be able to”, “be capable of”, “but not limited to”, “capability of”, “capability to”, “easy”, “effective”, “if practical”, “normal”, “provide for”, “timely”...</p>
Critical Area	Software Development Environment
Application	<p>Applicable to all MDA software development programs.</p> <p>Collected by software build and major component from Preliminary Design Review to Software Formal Qualification Test.</p> <p>Answers the question:</p> <p>Is the intent of the software requirements clearly communicated?</p>
Data Primitives Collected	<p>a. Total Software Requirements (monthly).</p> <p>b. Software Requirements with Ambiguous Phrase (monthly).</p>
Aggregate Values Calculated	<p><i>Requirements Ambiguity Percentage</i></p> $= \left[\frac{\text{Software Requirements with Ambiguous Phrase}}{\text{Total Software Requirements}} \right] \times 100$
Scoring Criteria	<p>Requirements Ambiguity</p> <p>GREEN: $\leq 30\%$ (pre-Critical Design Review (CDR)); $\leq 10\%$ (post-CDR)</p> <p>YELLOW: $30\% < \text{Requirements Ambiguity} \leq 40\%$ (pre-CDR)</p> <p>$10\% < \text{Requirements Ambiguity} \leq 20\%$ (post-CDR)</p> <p>RED: $> 40\%$ (pre-CDR); $> 20\%$ (post-CDR)</p>



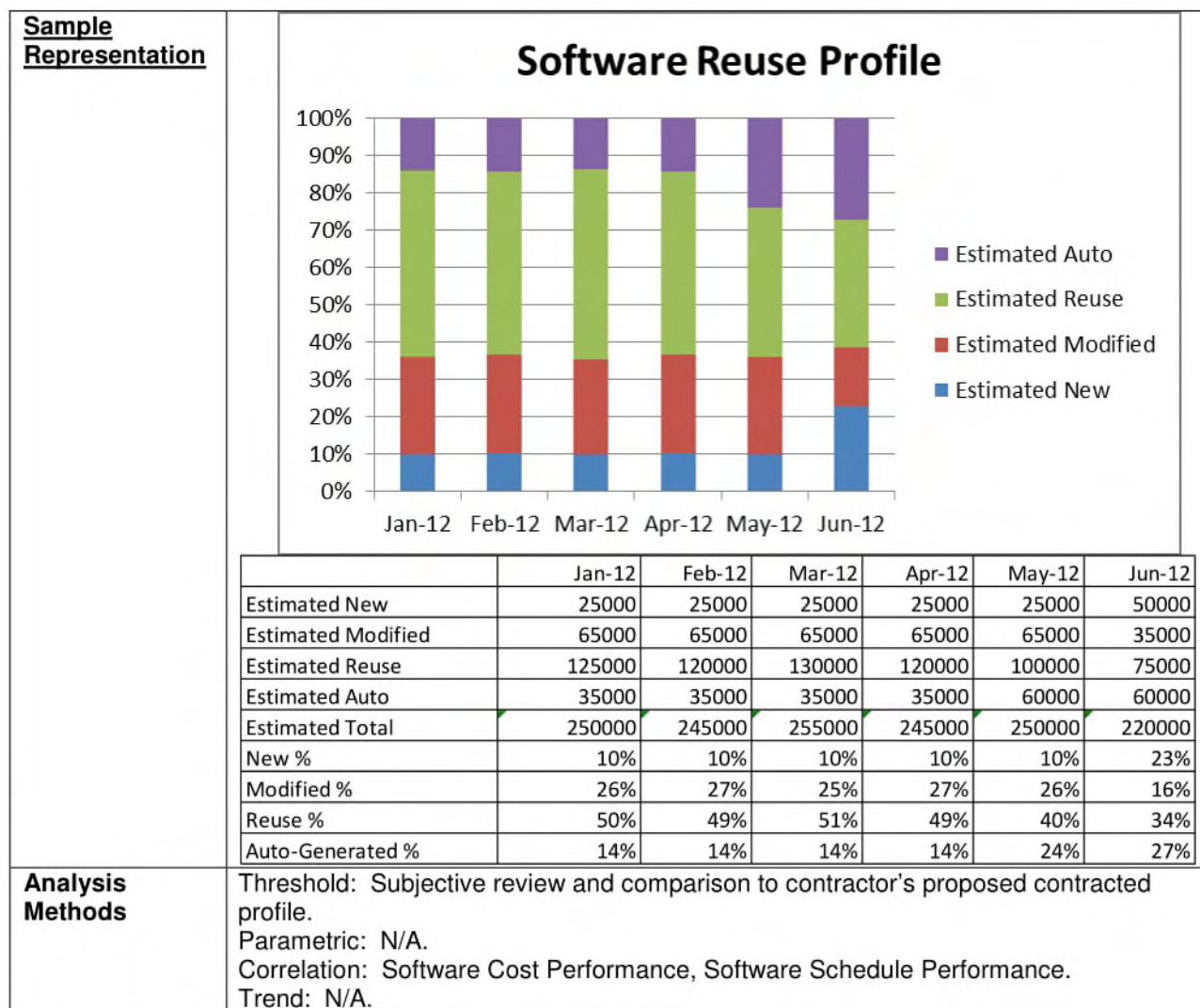
B.4.8.3 Software Requirements Incompleteness

Description	<p>The Software Requirements Incompleteness indicator identifies the level of uncertainty in the definition of the software requirements. Requirements incompleteness can lead to slips in schedule and increased costs to complete the requirements outside of the normal development cycle. The phrases identified for the Software Requirements Incompleteness indicator are listed below:</p> <p>"TBD", "TBA", "TBS", "To Be Determined", "To Be Added", "To Be Supplied"</p>
Critical Area	Software Development Environment
Application	<p>Applicable to all MDA software development programs.</p> <p>Collected by software build and major component from Preliminary Design Review to Software Formal Qualification Test.</p> <p>Answers the question:</p> <p>Are the software requirements completely defined?</p>
Data Primitives Collected	<p>a. Total Software Requirements (monthly).</p> <p>b. Software Requirements with Incompleteness Phrase (monthly).</p>
Aggregate Values Calculated	<p><i>Requirements Incompleteness Percentage</i></p> $= \left[\frac{\text{Software Requirements with Incompleteness Phrase}}{\text{Total Software Requirements}} \right] \times 100$
Scoring Criteria	<p>Requirements Incompleteness</p> <p>GREEN: ≤ 30% (pre-Critical Design Review (CDR)); ≤ 10% (post-CDR)</p> <p>YELLOW: 30% < Requirements Incompleteness ≤ 40% (pre-CDR) 10% < Requirements Incompleteness ≤ 20% (post-CDR)</p> <p>RED: > 40% (pre-CDR); >20% (post-CDR)</p>



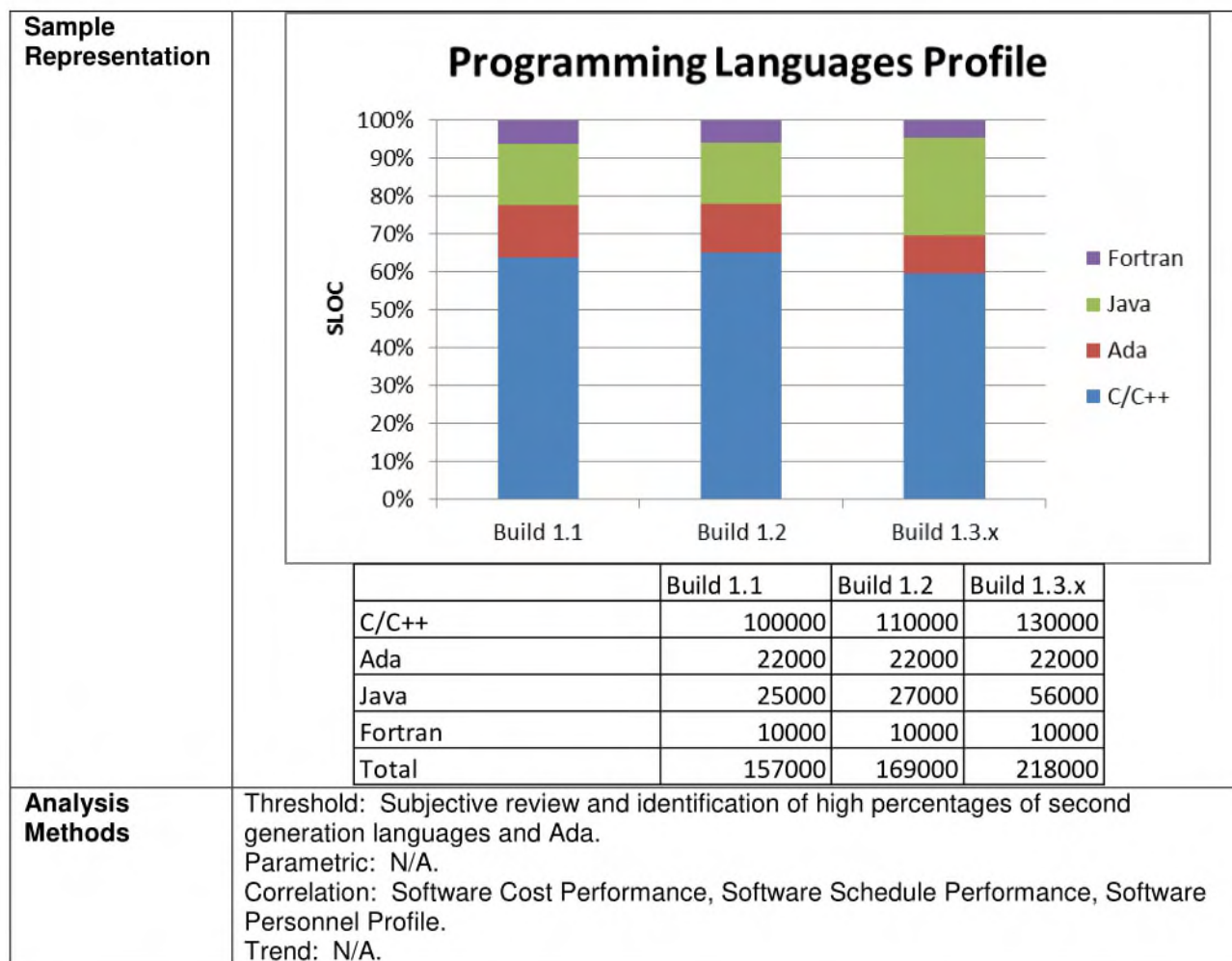
B.4.8.4 Software Reuse Profile

Description	The Software Reuse Profile indicator identifies the amount of software reused, modified, and auto-generated in the code base. Overestimations of reuse and other productivity measures are common in software development, and can lead to cost and schedule overruns as proposed reuse code is implemented as new code. The Software Profile provides insight into the code base and how well it is implementing aspects of reuse and other productivity measures.
Critical Area	Software Development Environment
Application	Applicable to all MDA software development programs. Collected by software build and major component from Requirements Analysis to Software Formal Qualification Test. Answers the question: Is the software development utilizing reuse and other productivity measures effectively?
Data Primitives Collected	a. Estimated New Source Lines of Code (SLOC) (monthly). b. Estimated Modified SLOC (monthly). c. Estimated Reuse SLOC (monthly). d. Estimated Auto-Generated SLOC (monthly).
Aggregate Values Calculated	a. Estimated Total SLOC = New + Modified + Reuse + Auto-Generated b. New % = (New / Total) × 100 c. Modified % = (Modified / Total) × 100 d. Reuse % = (Reuse / Total) × 100 e. Auto-Generated % = (Auto-Generated / Total) × 100
Scoring Criteria	There is no scoring criteria for Software Reuse Profile



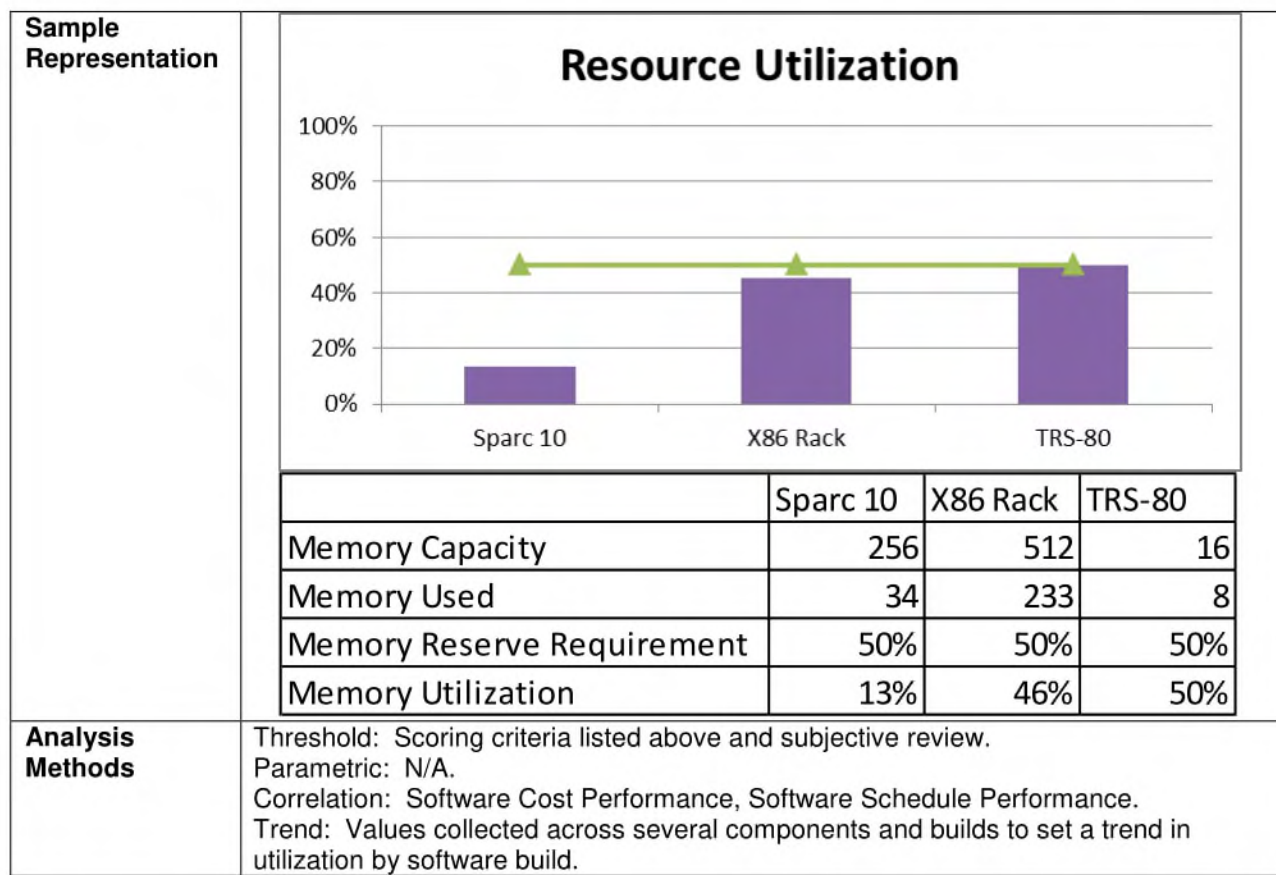
B.4.8.5 Programming Languages Profile

Description	The Programming Languages Profile indicator identifies the different programming languages used in the code base. Use of archaic and unsupported languages can cause impacts to cost and schedule as it is difficult to hire personnel to support the language or find development tools to create and maintain it. The Programming Languages Profile provides insight into the code base and how it is developed by language.
Critical Area	Software Development Environment
Application	Applicable to all MDA software development programs. Collected by software build and major component at major milestone reviews. Answers the question: Is the software development developed using modern, tool supported languages?
Data Primitives Collected	Estimated Total Source Lines of Code (SLOC) (by individual language).
Aggregate Values Calculated	Estimated Total SLOC % (by individual language)
Scoring Criteria	There is no scoring criteria for Programming Languages Profile



B.4.8.6 Resource Utilization

Description	The Resource Utilization indicator is used to monitor the utilization of computer resources in the areas of computer memory, computer storage, network throughput, and processor load against the target computer configuration. Resource Utilization should be measured at worse case (peak) in an operationally representative environment.
Critical Area	Software Development Environment
Application	<p>Applicable to all MDA software development programs.</p> <p>Collected by software target resource quarterly or as required.</p> <p>Answers the questions:</p> <ol style="list-style-type: none"> Is there sufficient margin in the target configuration memory for extended program use and growth? Is there sufficient margin in the target configuration storage for additional storage requirements? Is the target network throughput sufficiently controlled to avoid throttling? Are the computer processors allowed enough margin for growth and additional use?
Data Primitives Collected	<ol style="list-style-type: none"> Target Memory Capacity in megabytes (MB) (by resource) Memory Used in MB (by resource). Memory Reserve Requirement % (by resource). Target Mass Storage Capacity in MB (by resource). Mass Storage Used in MB (by resource). Mass Storage Reserve Requirement % (by resource). Target Network Capacity in kilobytes per second (kB/s) (by resource). Network Usage in kB/s (by resource). Network Reserve Requirement % (by resource). Target Processor Capacity in Millions Of Instructions Per Second (MIPS) (by resource). Processor Usage in MIPS (by resource). Processor Reserve Requirement % (by resource).
Aggregate Values Calculated	<ol style="list-style-type: none"> Memory Utilization (by resource)% = (Memory Used / Memory Capacity) × 100 Storage Utilization (by resource)% = (Storage Used / Storage Capacity) × 100 Network Utilization (by resource)% = (Network Usage / Network Capacity) × 100 Processor Utilization (by resource)% = (Processor Usage / Processor Capacity) × 100
Scoring Criteria	<p>Resource Utilization</p> <p>GREEN: Any Utilization ≤ Reserve Requirement</p> <p>YELLOW: Any Utilization > Reserve Requirement by 10% or less</p> <p>RED: Any Utilization > Reserve Requirement by more than 10%</p>



B.4.8.7 Cyclomatic Complexity

Description	The Cyclomatic Complexity indicator is used to indicate the complexity of a software program through the measure of the number of independent paths in the source code. Cyclomatic Complexity uses a control flow graph of the software with nodes representing groups of functions and edges representing the logical paths of the program. High cyclomatic complexity values can be correlated to higher defect occurrences and difficulty in code maintenance and reusability. Many tools for measuring cyclomatic complexity are commercially available.
Critical Area	Software Development Environment
Application	Applicable to all MDA software development programs. Collected by software build, major component, and software modules from Code and Unit Testing to software release. Answers the questions: a. Is the software being coded efficiently and with elegance? b. Will the software be difficult to maintain and reuse? c. What modules are likely to have defects due to complexity?
Data Primitives Collected	a. Number of edges (by module). b. Number of nodes (by module). c. Number of exit nodes (by module). d. Total number of software modules (by major component).
Aggregate Values Calculated	a. Cyclomatic Complexity (by module) = Edges – Nodes + Exit Nodes b. Number of Extreme Cyclomatic Complexity Modules (by module) = Number of Modules where Cyclomatic Complexity ≥ 15 c. Number of Distressing Cyclomatic Complexity Modules (by module) = Number of Modules where Cyclomatic Complexity ≥ 10 and < 15 d. Component Extreme Complexity % = (Number of Extreme Cyclomatic Complexity Modules / Total number of software modules) $\times 100$ e. Component Distressing Complexity % = (Number of Distressing Cyclomatic Complexity Modules / Total number of software modules) $\times 100$
Scoring Criteria	Component Complexity % GREEN: Component Extreme Complexity % = 0% AND Component Distressing Complexity % $< 10\%$ YELLOW: Component Extreme Complexity % = 0% AND $10\% \leq$ Component Distressing Complexity % $< 20\%$ RED: Component Extreme Complexity % $> 0\%$ OR Component Distressing Complexity % $\geq 20\%$

Sample Representation	<div><h3>Cyclomatic Complexity</h3><table><caption>Cyclomatic Complexity Data</caption><thead><tr><th>Component</th><th>Extreme %</th><th>Distressing %</th></tr></thead><tbody><tr><td>Component 1</td><td>13%</td><td>0%</td></tr><tr><td>Component 2</td><td>20%</td><td>0%</td></tr><tr><td>Component 3</td><td>8%</td><td>0%</td></tr><tr><td>Component 4</td><td>60%</td><td>0%</td></tr><tr><td>Component 5</td><td>18%</td><td>6%</td></tr></tbody></table></div> <table><thead><tr><th></th><th>Component 1</th><th>Component 2</th><th>Component 3</th><th>Component 4</th><th>Component 5</th></tr></thead><tbody><tr><td>Total Modules</td><td>15</td><td>20</td><td>13</td><td>5</td><td>17</td></tr><tr><td>Number Extreme</td><td>2</td><td>4</td><td>1</td><td>3</td><td>3</td></tr><tr><td>Number Distressing</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr><tr><td>Extreme %</td><td>13%</td><td>20%</td><td>8%</td><td>60%</td><td>18%</td></tr><tr><td>Distressing %</td><td>0%</td><td>0%</td><td>0%</td><td>0%</td><td>6%</td></tr></tbody></table> <table><thead><tr><th></th><th colspan="3">Component 1</th></tr><tr><th></th><th>Module 1</th><th>Module 2</th><th>Module 3</th></tr></thead><tbody><tr><td>Edges</td><td>15</td><td>20</td><td>28</td></tr><tr><td>Nodes</td><td>12</td><td>10</td><td>20</td></tr><tr><td>Exit Nodes</td><td>1</td><td>1</td><td>2</td></tr><tr><td>Total Modules</td><td>3</td><td>3</td><td>3</td></tr><tr><td>Cyclomatic Complexity</td><td>4</td><td>11</td><td>10</td></tr><tr><td>Number Extreme</td><td>2</td><td></td><td></td></tr><tr><td>Number Distressing</td><td>0</td><td></td><td></td></tr><tr><td>Extreme %</td><td>67%</td><td></td><td></td></tr><tr><td>Distressing %</td><td>0%</td><td></td><td></td></tr></tbody></table>	Component	Extreme %	Distressing %	Component 1	13%	0%	Component 2	20%	0%	Component 3	8%	0%	Component 4	60%	0%	Component 5	18%	6%		Component 1	Component 2	Component 3	Component 4	Component 5	Total Modules	15	20	13	5	17	Number Extreme	2	4	1	3	3	Number Distressing	0	0	0	0	1	Extreme %	13%	20%	8%	60%	18%	Distressing %	0%	0%	0%	0%	6%		Component 1				Module 1	Module 2	Module 3	Edges	15	20	28	Nodes	12	10	20	Exit Nodes	1	1	2	Total Modules	3	3	3	Cyclomatic Complexity	4	11	10	Number Extreme	2			Number Distressing	0			Extreme %	67%			Distressing %	0%		
	Component	Extreme %	Distressing %																																																																																																
	Component 1	13%	0%																																																																																																
	Component 2	20%	0%																																																																																																
	Component 3	8%	0%																																																																																																
	Component 4	60%	0%																																																																																																
	Component 5	18%	6%																																																																																																
		Component 1	Component 2	Component 3	Component 4	Component 5																																																																																													
	Total Modules	15	20	13	5	17																																																																																													
	Number Extreme	2	4	1	3	3																																																																																													
Number Distressing	0	0	0	0	1																																																																																														
Extreme %	13%	20%	8%	60%	18%																																																																																														
Distressing %	0%	0%	0%	0%	6%																																																																																														
	Component 1																																																																																																		
	Module 1	Module 2	Module 3																																																																																																
Edges	15	20	28																																																																																																
Nodes	12	10	20																																																																																																
Exit Nodes	1	1	2																																																																																																
Total Modules	3	3	3																																																																																																
Cyclomatic Complexity	4	11	10																																																																																																
Number Extreme	2																																																																																																		
Number Distressing	0																																																																																																		
Extreme %	67%																																																																																																		
Distressing %	0%																																																																																																		
Analysis Methods	<p>Threshold: Scoring criteria listed above and subjective review.</p> <p>Parametric: Utilization of McCabe COTS analysis tools.</p> <p>Correlation: Software Cost Performance, Software Schedule Performance, Software Defect Profile, Software Defect Closure, Programming Language Profile, First Time Quality of Software.</p> <p>Trend: Values collected across several components and builds to set a trend in utilization by software build and major component.</p>																																																																																																		

13 June 2014

MDA-QS-001-MAP-Rev B

APPENDIX (C)

Workmanship Requirements

Table of Contents

C.1	Workmanship Standard Criteria	C-5
C.2	Connector Mating and Demating	C-5
C.3	General Torque Requirements.....	C-6

C.1 Workmanship Standard Criteria

The contractor shall use approved workmanship standards. Workmanship standards promote standardized designs and fabrication practices to enhance assembly, durability, and reliability; and restrict the use of designs and manufacturing processes known to reduce those qualities. Contractor's approved workmanship standards shall be traceable to Military and Industry specifications or standards and approved by the contractor's cognizant discipline (design, engineering, manufacturing, and quality) organizations.

Each workmanship standard shall contain at least the following information:

- a. Design criteria.
- b. Tooling.
- c. Detailed acceptance or rejection criteria.
- d. Personnel training and qualification requirements.

C.2 Connector Mating and Demating

The contractor shall adhere to the following practices and precautions in mating and demating connectors:

- a. Prior to connector mate/demate operations, verify the circuit has been de-energized.
- b. Electrostatic protection procedures shall be observed.
- c. Each half of each flight connector shall be inspected for cleanliness, particulate contamination, shell damage, misalignment of backshell torque stripe, broken or missing grounding fingers, interfacial riser damage (tears or gouges), broken bayonets, damaged or missing contact retainer clips, recessed contacts, and pin alignment before mating and after demating. Inspect connectors using 4X magnification minimum (10X preferred) under adequate lighting conditions and record inspection results on the planning documentation.
- d. All flight qualified, ac/dc power interface and test equipment connectors that mate with flight and support equipment connectors shall be protected against damage and contamination during mating and demating operations, and when they are in a demated condition.
- e. Caution shall be applied to mating and demating operations to preclude damage to connectors. In some cases a demating tool may be utilized.
- f. Harness connectors mated to test tees or breakout boxes shall be provided with stress relief to restrict flexing of connectors and cables. Breakout boxes shall be grounded to facility ground prior to mating harness connectors to either ground support equipment or flight hardware.
- g. Mate/demate operations between the flight hardware, support equipment connectors, system test equipment, and also in final assembly shall be performed by trained and qualified personnel. Personnel mating and demating flight connectors must understand the mechanical mating/demating method of the specific connector, before starting the actual mating or demating process.
- h. The use of connector savers is required. Connector savers shall meet the same requirements as a flight connector and shall be clearly marked.
- i. Interfacial seals, which are not bonded to the connector shall be examined and, if necessary, replaced with new, clean seals prior to final mating.

- j. A log of mate and demate operations and a bent pin log shall be maintained to document material history for flight connectors. Each mate and each demate of a flight connector shall be recorded in the mate/demate log. This applies to connectors inside the equipment as well as external connectors. This also applies when flight connectors are mated with and demated from connector savers as well as other flight connectors.
- k. Flight connectors shall be torqued as specified on engineering documentation.
- l. Electrostatic discharge (ESD) protective caps shall be installed on exposed connectors of harnesses that are attached to ESDS hardware. Insure the protective cap is clean, both inside and outside, and store unused protective caps in a clean zip-lock bag.
- m. Flight connectors lockwired shall be secured to vehicle structure in accordance with engineering documentation.
- n. Flight harnesses shall have sufficient slack between last attach point, when extended taut, to ensure quick-disconnect mechanism engagement release of flight connectors as specified on engineering documentation.

C.3 General Torque Requirements

The extensive use of bolts, studs, and nuts as fastening elements and an avoidable quality problem history makes proper selection and tightening of fasteners essential. The contractor shall ensure that fastener selection and tightening meet or exceed industry best practices and the following generalized requirements derived from industry specifications and standards.

- a. Holes shall be verified as deburred before fasteners are installed.
- b. No lubricant or sealant shall be applied to fasteners or threads unless it is specifically called out on the engineering drawing.
- c. Threaded fastening system hardware shall be inspected prior to installation to verify that part number(s), cleanliness, and orientation are in accordance with the engineering documentation.
- d. Locking torque shall be measured during installation and verified to be within the minimum-maximum range.
- e. Fasteners removed shall be reinstalled using the same procedures as for new fasteners. Fasteners shall be examined for wear or deformation before being reinstalled.
- f. Tools and instruments used to install fastening system hardware shall be used within their design and calibration ranges.
- g. Torque instruments should be chosen so the torque (running or final assembly) being measured or controlled is between 20 and 90 percent of the instruments' full-scale torque.
- h. All torque wrenches shall be verified to be in calibration before they are used.
- i. If a calibrated tool or instrument is dropped, struck, or otherwise damaged or suspected of being out of calibration, the calibration shall be re-verified before further use.
- j. The tool or instrument name, serial number, calibration due date, and torque value shall be recorded on the planning for traceability.
- k. Fasteners shall be tightened to the installation torque specified by the engineering drawing.

- l. The engineering documentation shall specify the installation torque range or specify an applicable standard that defines the installation torque range.
- m. The engineering documentation shall clearly identify when the installation torque is the torque above running torque. Running torque shall be recorded on the planning documentation.
- n. Personnel installing fastening system hardware shall be qualified through experience and formal training per program, project, or organization specific quality processes.
- o. Tightening sequence shall be a star pattern unless system design requirements require alternate tightening scheme. A verification check shall be performed either in a clockwise or counter clockwise direction to ensure all fasteners are tight.
- p. Mechanical locking features shall be verified by visual inspection after installation.
- q. Adhesive locking features dependent upon substrate or configuration for cure shall be verified by torque measurements on witness coupons that are representative of and processed with hardware being verified.
- r. All other adhesive locking features shall be verified using cure samples processed at the time of application/processing.
- s. Quality shall witness and record in planning documentation all torquing operations when safety and mission critical items are installed in flight systems.

APPENDIX (D)

Acronyms

Acronyms

ACWP	Actual Cost of Work Performed
ACWS	Actual Cost Work Scheduled
ADT	Administrative Delay Time
AFSPC	Air Force Space Command
Ai	Inherent Availability
AIAA	American Institute of Aeronautics and Astronautics
Ao	Operational Availability
AECA	Arms Export Control Act
ANSI	American National Standards Institute
ASIC	Application Specific Integrated Circuit
ASR	Alternative Systems Review
AVI	Allocated Volatility Index
BAC	Budget at Completion
BCWP	Budgeted Cost of Work Performed
BCWS	Budgeted Cost of Work Scheduled
BIT	Built-In Test
BITE	Built-In Test Equipment
BMD	Ballistic Missile Defense
BMD SS	Ballistic Missile Defense System Specification
BMDS	Ballistic Missile Defense System
C2BMC	Command and Control, Battle Management, and Communications
CARD	Cost Analysis Requirements Description
CCB	Configuration Control Board
CCP	Contamination Control Program
CDA	Critical Design Assessments
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CI	Configuration Item
CM	Configuration Management
CMMI	Capability Maturity Model Integration
COCOMO	Constructive Cost Model
CONOPS	Concept of Operations
COTS	Commercial-Off-The Shelf
CPI	Cost Performance Index
CPU	Central Processing Unit
CSA	Configuration Status Accounting
CSI	Cost Schedule Index
CV	Cost Variance
DCE	Defect Containment Effectiveness
DCMA	Defense Contract Management Agency
DDTC	Directorate of Defense Trade Controls
DM	Data Management
DOD	Department of Defense
DODI	Department of Defense Instruction
DOL	Department of Labor
DVI	Derived Volatility Index
EAC	Estimate At Completion
ECP	Engineering Change Proposal
EKSLOC	Equivalent Thousand Source Lines of Code
EP	Equivalent Personnel

ESD	Electrostatic Discharge
ESDS	Electrostatic Discharge Sensitive
ESLOC	Equivalent Source Lines of Code
ESS	Environmental Stress Screening
EV	Earned Value
FAR	Federal Acquisition Regulation
FCA	Functional Configuration Audit
FD	Fault Detection
FEA	Finite Element Analysis
FI	Fault Isolation
FMECA	Failure Modes, Effects, and Criticality Analysis
FOD	Foreign Object Damage / Foreign Object Debris
FOE	Foreign Object Elimination
FOR	Flight Operations Review
FPGA	Field Programmable Gate Array
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FRB	Failure Review Board
FTA	Fault Tree Analysis
FTP	File Transfer Protocol
FTS	Flight Termination Systems
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFM	Government Furnished Materials
GIDEP	Government Industry Data Exchange Program
GSE	Ground Support Equipment
GSI	Government Source Inspection
HALT	Highly Accelerated Life Test
HASS	Highly Accelerated Stress Screen
HCI	Hardness Critical Items
HMMP	Hazardous Materials Management Plan
IAW	In Accordance With
ICD	Interface Control Documents and Drawings
ICN	Interface Change Notice
ICP	Interface Control Plan
ICWG	Interface Control Working Group
ID	Interface Documentation
IDD	Interface Design Description
IDE	Integrated Digital Environment
IED	Independent Estimate of Delivery
IEEE	Institute of Electrical and Electronics Engineers
IER	Information Exchange Requirement
IG	Inspector General
IMS	Integrated Master Schedule
IPC	Institute for Interconnecting and Packaging Electronic Circuits
IPP	Isolation Protection Profile
IPT	Integrated Product Team
IRIG	Inter-Range Instrumentation Group
IRS	Interface Requirements Specification
ISO	International Organization for Standardization
ISSPP	Integrated System Safety Program Plan
ITAR	International Traffic in Arms Regulations
ITR	Initial Technical Review

IUID	Item Unique Identification
IV&V	Independent Verification and Validation
KPI	Key Personnel Index
KSLOC	Thousand Source Lines of Code
LCSP	Life Cycle Sustainment Plan
LOE	Level of Effort
LRE	Latest Revised Estimate
LRR	Launch Readiness Review
M&S	Modeling and Simulation
MAIP	Mission Assurance Implementation Plan
MAP	MDA Assurance Provisions
MAR	MDA Assurance Representatives
MB	Megabyte
MDA	Missile Defense Agency
MDALL	MDA Lessons Learned
MGI	Mandatory Government Inspection
MIL	Military
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MIPS	Millions of Instructions Per Second
MLDT	Mean Logistics Delay Time
MMH	Maintenance Man Hours
MOR	Mission Operations Review
MR	Maintenance Ratio
MRB	Material Review Board
MRT	Mean Repair Time
MSDS	Material Safety Data Sheet
MSMDT	Mean Schedule Maintenance Downtime
MTBCF	Mean Time Between Critical Failure
MTTR	Mean Time to Repair
MTTRF	Mean Time to Restore Functions
NDI	Non-Developmental Item
NKPI	Non-Key Personnel Index
O&SHA	Operations and Support Hazard Analysis
OSH	Occupational Safety and Health
OSHA	Occupational Safety and Health Act/Administration
PCA	Physical Configuration Audit
PCB	Program Change Board
PCE	Phase Containment Effectiveness
PDA	Preliminary Design Assessments
PDR	Preliminary Design Review
PDUSD(AT&L)	Principal Deputy Under Secretary of Defense Acquisition, Technology and Logistics
PDWR	Predicted Development Work Remaining
PER	Pre-Environmental Review
PESHE	Programmatic Environmental, Safety, and Occupational Health Evaluation
PFMEA	Process Failure Modes and Effects Analysis
PLD	Programmable Logic Device
PM	Preventive Maintenance
PMAP	Parts, Materials, and Processes Mission Assurance Plan
PMP	Parts, Materials, and Processes

PMPCB	Parts, Materials, and Processes Control Board
PMPCP	Parts, Materials, and Processes Control Program
PR	Percent Rework
PRR	Production Readiness Review
PSR	Pre-Shipment Review
PTIP	Product Test and Inspection Plan
QA	Quality Assurance
QMS	Quality Management System
QS	Quality, Safety, and Mission Assurance Directorate
QSMa	Quality, Safety, and Mission Assurance
RAM	Requirements Applicability Matrix
RCC	Range Commanders Council
RE	Responsible Engineers
RF	Radio Frequency
RH	Relative Humidity
RM&A	Reliability, Maintainability, and Availability
RMP	Risk Management Plan
ROM	Read-Only Memory
RPI	Rework Planning Index
RQT	Reliability Qualification Testing
RVI	Requirements Volatility Index
SAE	Society of Automotive Engineers
SAR	Safety Assessment Report
SC	Software Components
SCCS	Safety Critical Computing System
SCCSF	Safety Critical Computing System Functions
SCI	Software Configuration Item
SCM	Software Configuration Management
SDP	Software Development Plan
SEP	Systems Engineering Plan
SEMP	Systems Engineering Management Plan
SFR	System Functional Review
SLOC	Source Lines of Code
SMC	Space and Missile Systems Center
SOW	Statement of Work
SPI	Schedule Performance Index
SQA	Software Quality Assurance
SRPP	Software Reliability Program Plan
SRR	System Requirements Review
SRS	Software Requirements Stability
SSPP	System Safety Program Plan
SSR	Software Specification Reviews
SSWG	System Safety Working Group
SU	Software Units
SV	Schedule Variance
SVD	Software Version Description
SVR	System Verification Review
SwSWG	Software Safety Working Group
TB	Technical Bulletin
TCE	Total Containment Effectiveness
TDP	Technical Data Package
TLYF	Test-Like-You-Fly

TMDE	Test, Measuring, and Diagnostic Equipment
TMDES	Test, Measuring, and Diagnostic Equipment and Standards
TOC	Total Ownership Cost
TPM	Technical Performance Measurement
TRR	Test Readiness Review
TSPI	To-Complete Schedule Performance Index
TT&E	Test, Training, and Exercise

USML	United States Munitions List
------	------------------------------

V&V	Verification and Validation
VAC	Variance at Completion
VV&A	Verification, Validation, and Accreditation

MDA Organizations

MDA/D – Director, Missile Defense Agency

MDA/BC – Director for C2BMC

MDA/CR – Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance

MDA/DX – Executive Director

MDA/DA – Deputy for Acquisition Management

MDA/DE – Director for Engineering

MDA/DT – Director for Test

MDA/DV – Advanced Technology

MDA/GD – Global Deployment

MDA/QS – Director for Quality, Safety and Mission Assurance

APPENDIX (E)

Definitions

Definitions

For the purposes of this document the following definitions apply.

Acceptance: The act of an authorized representative of the Government by which the Government, for itself, or as agent of another, assumes ownership of existing identified supplies tendered, or approves specific services rendered, as partial or complete performance of the contract or work authorization.

Acceptance Test: A test conducted under specified conditions by, or on behalf of the Government, using delivered or deliverable items, in order to determine the item's compliance with specified requirements.

Accreditation: The official certification that a model, simulation, or federation of models and simulations and its associated data are acceptable for use for a specific purpose.

Allocated Baseline: The initially approved documentation describing an item's functional, interoperability, and interface characteristics that are allocated from those of a system or a higher level configuration item, interface requirements with interfacing configuration items, additional design constraints, and verification required to demonstrate achievement of those specified characteristics.

Assembly: A number of parts or subassemblies or any combination thereof joined together to form a specific function and capable of disassembly.

Autonomous Software Control: Software control that does not require human intervention to process data or issue commands. In this sense, a fault, failure, or defect in the software will lead to a hazard or a mishap over which the operator has no control.

Availability: A measure of the degree to which an item is in an operable state and can be committed at the start of a mission when the mission is called for at an unknown (random) point in time. See Inherent Availability (Ai) and Operational Availability (Ao).

Baseline: (1) An agreed to description of the attributes of a product or item, at a point in time, which serves as a basis for defining change; (2) An approved and released document, or a set of documents, each of a specific revision, the purpose of which is to provide a defined basis for managing change; (3) The currently approved and released configuration documentation; and (4) A released set of files comprising a software version and associated configuration documentation.

Battleshort (Safety Arc): The capability to bypass certain safety features in a system to ensure completion of a mission without interruption due to the safety feature. Bypassed safety features include such items as circuit current overload protection and thermal protection.

Bit Inverter/Bit Flipper: A bit inverter or bit flipper is a device or software application whose intended function includes modifying a message in such a way as to change the source identity, operations mode (e.g., test, training, or operation) or original sender intent, in order to defeat (or spoof) filters or rules that would otherwise prevent the message from being processed by a given application.

Capability Development Document: A document that captures information necessary to develop a proposed program, normally using an evolutionary acquisition strategy. The Capability Development Document outlines an affordable increment of militarily useful, logistically supportable, and technically mature capability. The Capability Development Document may define multiple increments if there is sufficient definition of the performance attributes (key performance parameters, key system attributes, and other attributes) to allow approval of multiple increments. The Capability Development Document supports a Milestone B decision review per DOD Acquisition Guide.

Capability Production Document: A document that addresses production elements specific to a single increment of an acquisition program. The Capability Production Document defines an increment of

militarily useful, logistically supportable, and technically mature capability that is ready for a production decision. The Capability Production Document must be validated and approved prior to a Milestone C decision review per DOD Acquisition Guide.

Chargeable Failure: Any independent relevant failure of Contractor or Government Furnished Equipment or incorporated equipment (i.e., hardware, software, crew/operator, technical documentation, maintenance personnel, training, support items, accident, hardware BIT, software BIT, and firmware).

Command Media: The contractor's specifications, engineering drawings, build paper, test procedures, detailed process instructions, design manuals and other documentation generated to comply with Statement of Work (SOW) requirements that ensure repeatability in products produced and services provided; also included are contractor's corporate policies, procedures and best practices that govern design margins, promote reliability, and infuse corporate knowledge into improving products and services.

Commercial-Off-The-Shelf Items: Products or equipment developed by industry for sale in the general commercial market place. Commercial items may include modifications, provided modifications are either: (1) Of a type customarily available in the commercial marketplace; or (2) Of a type not customarily available in the commercial marketplace, which do not alter the non-governmental function, essential physical characteristics of an item or component, or change the purpose of a process.

Configuration: (1) The performance, functional, and physical attributes of an existing or planned product, or a combination of products. (2) One of a series of sequentially created variations of a product.

Configuration Audit: Product configuration verification accomplished by inspecting documents, products and records; and reviewing procedures, processes, and systems of operation to verify that the product has achieved its required attributes (performance requirements and functional constraints) and the product's design is accurately documented.

Configuration Control: (1) A systematic process which ensures changes to released configuration documentation are properly identified, documented, evaluated for impact, approved by an appropriate level of authority, incorporated, and verified. (2) The configuration management activity concerning systematic proposal, justification, evaluation, coordination, and disposition of proposed change, and implementation of all approved and released changes into (a) applicable configurations of a product; (b) associated product information; and (c) supporting and interfacing products and their associated product information.

Configuration Control Board (CCB): A board composed of technical and administrative representatives who recommend approval or disapproval of proposed engineering changes to a Configuration Item's (CI) current approved configuration documentation. The board also recommends approval or disapproval of proposed waivers and deviations from a CI's current approved configuration documentation.

Configuration Documentation: Technical information, the purpose of which is to identify and define a product's performance, architectural, functional, and physical attributes (e.g., specifications, drawings, and version descriptions).

Configuration Identification: Configuration identification includes selection of Configuration Items (CI); determination of types of configuration documentation required for each CI; issuance of numbers and other identifiers affixed to CIs and technical documentation that defines the CI's configuration, including internal and external interfaces; release of CIs and their associated configuration documentation; and establishment of configuration baselines for CIs.

Configuration Item (CI): A configuration item is an aggregation hardware, software, or firmware that satisfies an end use function and is designated by the Government for separate configuration management.

Configuration Management (CM): A management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

Configuration Status Accounting (CSA): The configuration management activity concerning capture and storage of, and access to, configuration information needed to manage products and product information effectively, including: (1) A record of the approved configuration documentation and identification numbers; (2) The status of proposed changes, deviations, and waivers to the configuration; (3) The implementation status of approved changes; and (4) The configuration of all units of the configuration item in the operational inventory.

Configuration Verification: The action of verifying that the product has achieved its required attributes (performance requirements and functional constraints) and the product's design is accurately documented.

Contractor Acquired Property: Property obtained or otherwise provided by the contractor for performing a contract.

Controlled Items: An assembly or subassembly, known or suspected to be subject to a rate of deterioration with operation sufficient to cause reliability degradation during service life. Controlled items require the recording of operating data for reliability evaluation or preventative maintenance purposes. Operating data to be tracked includes operating time, operating cycle, or power turn-on, as applicable to the item. The term "controlled items" excludes items that deteriorate solely based on calendar age (see "limited life items").

Critical Event: An event that includes major program milestones, mission assurance reviews (e.g., Mission Readiness Review, Pre-Environmental Review, or Pre-Shipment Review) and flight or ground tests.

Critical Lifts: Lifts where a failure or loss of control could result in loss of life, loss of or damage to flight hardware, or a lift involving special high dollar items, such as satellites, missile assemblies and components, consoles, one-of-a-kind articles, or major facility components, where loss would have serious programmatic or institutional impact. Critical lifts also include lifting of personnel with a crane, lifts where personnel are required to work under a suspended load, and operations with special personnel and equipment safety concerns beyond normal lifting hazards.

Critical Moves: A move to critical hardware involving special high dollar items such as payloads, missile assemblies, subassemblies, components, or one-of-a-kind articles where loss or damage would have serious programmatic impact.

Deactivated Code: Source code or executable code for which there are no requirements in the current build, but which may be required in other builds, and for which the risk of removal is unacceptable.

Dead Code: Executable code for which there are no documented requirements. Also included is executable code for which the control structure does not allow execution.

Defect: Any nonconformance of the unit of product with specified requirements or any state or condition of nonconformance to requirements.

Derating: The reduction of applied load (or rating) of a device to improve reliability or to permit operation at high ambient temperatures.

Designed Safe State: A system state that provides the maximum degree of safety within the constraint of the current operational or logistic phase.

Devices: (1) A hardware item or assembly that can be further disassembled; and (2) A piece of equipment or a mechanism designed to serve a special purpose or to perform a special function.

Digital Data: Includes all product information and data prepared and maintained by electronic means and provided by electronic data access, interchange, transfer, or on electronic media.

Document Representation: (1) A set of digital files which, when viewed or printed together, collectively represent the entire document (e.g., a set of raster files or a set of IGES files). A document may have more than one document representation. (2) A document in a non-digital form (e.g., paper, punched card set, or stable-base drawing).

Emergent Behavior: System level behavior that is not explicitly predicted by system components' behavior, and is therefore unexpected to a designer or observer.

Energetics: A system that uses explosives, propellants, directed energy, pyrotechnics, initiating composition; or nuclear, biological, or chemical material for use in military operations.

Engineering Change: A change to current approved configuration documentation of a configuration item at any point in the item life cycle.

Establish and Maintain: Establish and maintain includes planning, developing, preparing, implementing, documenting, assessing, updating, and performing.

Fabrication: The process of converting raw materials into required material. It includes the functions of scheduling, inspection, quality control, and related processes.

Facility Location: The location where the purchased item is actually built or produced. This does not include the location of a vendor or a distributor who simply sells supplies that they do not produce.

Failure: An event in which an item does not perform one or more of its required functions within the specified limits under specified conditions. A failure can either be catastrophic (total loss of function) or out-of-tolerance (degraded function beyond specified limits due to such occurrences as part failure, detuning, misalignment, and maladjustment, which are often classified as faults).

Failure Modes and Effects Analysis: A procedure by which each credible failure mode of each item from a low indenture level to the highest is analyzed using inductive logic to determine effects on the system and to classify each potential failure mode in accordance with the severity of its effect.

Fault Tolerance: The ability of a system to continue functioning and preserve the integrity of data with certain faults present. Fault tolerance is a property which is designed into the system. It includes but is not limited to the following elements:

- a. **Fault Detection:** The ability to monitor system status and communication to identify out of tolerance conditions. Also, the ability to actively test for faults.
- b. **Fault Isolation:** The ability to minimize and mitigate the fault such that the effects are not propagated to other parts of the system which were not initially impacted.
- c. **Fault Recovery:** The ability to continue operations through redundant capability or through fallback to a system state prior to the fault.
- d. **Graceful Degradation:** In the event that recovery is not possible, graceful degradation is the ability to terminate a system function such that critical data are stored and hazards to personnel and equipment are not introduced.

Fault Tree Analysis: A process of reviewing and analytically examining a system or equipment in such a way as to emphasize the lower level fault occurrences, which directly or indirectly contribute to the major fault or undesired event. Fault tree analysis emphasizes a pictorial presentation and deductive logic.

Firmware: The combination of a discrete part and computer instructions, data, and/or logic that reside on the part. Firmware includes Field Programmable Gate Arrays (FPGA), Programmable Logic Devices (PLD), and Application Specific Integrated Circuits (ASIC).

Foreign Object Damage: Damage to product caused by a foreign object.

Foreign Object Debris: Foreign material which could potentially cause product damage or degraded performance.

Functional Baseline: The initially approved documentation describing a system's or item's functional, interoperability, and interface characteristics and the verification required to demonstrate achievement of those specified characteristics.

Functional Configuration Audit (FCA): The formal examination of functional characteristics of a configuration item, before acceptance, to verify that the item has achieved requirements specified in its functional and allocated baselined configuration documentation.

Government Furnished Property: Property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government furnished property also includes contractor acquired property if the contractor acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract.

Hardware: Products made of material and their components (e.g., mechanical, electrical, electronic, hydraulic, or pneumatic). Computer software and technical documentation are excluded.

Hazard: Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment. A hazard is a prerequisite to a mishap.

Highly Accelerated Life Test (HALT): A process that utilizes a step stress approach to subject a unit under test to thermal and vibration stresses of types and levels beyond what it may see in actual use, but which will rapidly induce failure modes, allowing them to be detected and corrected. The stresses applied include thermal extremes, extreme thermal ramp rates, 6 DoF (Degrees of Freedom) repetitive shock vibration, and combinations of these stresses.

Highly Accelerated Stress Screen (HASS): A production screen using the same accelerated techniques as HALT, but derated. Its purpose is to monitor the manufacturing process for deviations by screening production units.

Inherent Availability (Ai): Availability of a system with respect only to operating time and corrective maintenance. Ai ignores standby and delay times associated with preventive maintenance as well as administrative and logistics down time and may be calculated as the ratio of Mean Time Between Critical Failures (MTBCF) divided by the sum of MTBCF and Mean Time To Repair (MTTR), i.e., $A_i = MTBCF / (MTBCF + MTTR)$.

Interface: The performance, functional, and physical attributes required to exist at a common boundary.

Interface Control: The process of identifying, documenting, and controlling all performance, functional, and physical attributes relevant to the interfacing of two or more products provided by one or more organizations.

Interoperability: The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

Item Unique Identification (IUID): A system of marking items delivered to DOD with unique item identifiers that have machine readable data elements to distinguish an item from all other like and unlike items. For items that are serialized within the enterprise identifier, the unique item identifier shall include data elements of the enterprise identifier and a unique serial number. For items that are serialized within the part, lot, or batch number within the enterprise identifier, the unique item identifier shall include data elements of the enterprise identifier; original part, lot, or batch number; and serial number.

Key Characteristics: An attribute or feature of a material, part, assembly, installation, or system whose variation has a significant influence on product fit, performance, service life, or manufacturability and that requires specific actions for the purpose of controlling variation.

Legacy Design: A released design (i.e., hardware, software, or firmware) developed for the DOD and considered for use in MDA systems, subsystems, or assemblies because of a similar application. Legacy (aka: heritage) designs include a technical data package, design validation and verification records, reliability records, safety, and qualification records.

Life Cycle: A generic term relating to the entire period of concept refinement and technology development; system development and demonstration; production and deployment; operations and support; and disposal of a product.

Limited Life Items: A component, part, or material known or suspected to be subject to a rate of deterioration with calendar time sufficient to cause reliability degradation before installation or during service life. Limited life items require calendar age controls before acceptance to prevent use of over age components, parts, or materials and to provide a baseline for reliability evaluation or preventative maintenance purposes.

Maintainability: A measure of the ability of a system or subsystem to be retained in or restored to a specific condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each level of maintenance and repair. Maintainability is used to determine ease of access, spares variability, test equipment readiness, testability provisioning, accuracy of technical orders, and training requirements.

Material: Any substance used for production or fabrication of a product.

Mean Logistics Delay Time (MLDT): Indicator of the average time a system is awaiting maintenance and generally includes time for locating parts and tools; locating, setting up, or calibrating test equipment; dispatching personnel; reviewing technical manuals; complying with supply procedures; and awaiting transportation. The MLDT is largely dependent upon the logistics support structure and environment.

Mean Repair Time (MRT): The average on-equipment, off-equipment or both corrective maintenance times. It includes all maintenance actions needed to correct a malfunction, including preparing for test, troubleshooting, removing and replacing components, repairing, adjusting, re-assembly, alignment, adjustment, and checkout. The MRT does not include maintenance, supply or administrative delays. Note: MRT differs from the contractual term Mean Time to Repair (MTTR) in that it measures activities that occur in the operational environment.

Mean Time Between Critical Failure (MTBCF): Average time between failures that cause a loss of system function defined as "critical" by the subsystem or mission essential by the warfighter.

Mean Time to Repair (MTTR): Average time required to bring the system from a failed state to an operable state. Assumes maintenance personnel and spares are on hand. Typically includes isolation, remove and replacement of failed item(s), and checkout.

Mean Time to Restore Function (MTTRF): Average time required, as the result of critical failure, to restore a system to full operating status. It includes administrative and logistics delay times associated with restoring function following a critical failure.

MDA Program Offices: The executing “two-letter” Program Offices, (e.g., AB, TH, SN, TC, or GM) within MDA.

Mishap: An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Mission Assurance: (1) An engineering level assurance process performed over the program life cycle to identify and mitigate design, production, and test deficiencies that could affect mission success. (2) The disciplined application of general system engineering, risk management, quality, and management principles to achieve mission success. A disciplined mission assurance process has independent technical assessment as a cornerstone throughout the entire planning, design, development, fabrication, test, deployment, and support processes.

Mission Critical Failure: A failure or combination of failures, which prevents an item from performing a specified mission. Any fault, failure, or malfunction that results in the loss of any mission essential function. Critical failures do not always occur during mission time; they merely must or could cause mission impact. For the purpose of this document, mission time is defined as any time the system is required to perform its mission. Hardware and software failures, operator errors, and errors in technical orders that cause such a loss are normally counted as critical failures.

Mission Critical Item: A mission critical item, if defective, will prevent command and control, sensors, weapons, combat, or flight systems from achieving mission primary objectives. A failure of the mission critical item would affect system or personnel safety, mission success, or operational readiness. Examples of mission critical items include, but are not limited to: items having limited operating life (controlled items), one shot devices, items causing single points of failure, or items that cannot be tested before flight or use.

Nonconformance: The failure of a characteristic to conform to the requirements specified in the contract, drawings, specifications, or other approved product description.

Non-Developmental Item (NDI): (1) Any previously developed item of supply used exclusively for Government purposes by a federal agency, a State or local Government, or a foreign Government with which the United States has a mutual defense cooperation agreement. (2) Any item described in item (1) that requires only minor modifications or modifications of the type customarily available in the commercial marketplace in order to meet the requirements of the procuring department or agency. (3) Any item of supply being produced that does not meet the requirements of items (1) or (2) solely because the item is not yet in use.

Non-Volatile Memory: Types of memory that retain their contents when power is turned off.

Open System: A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered components to be used across a wide range of systems with minimal changes, to interoperate with other components on local and remote systems, and to interact with users in a style that facilitates portability.

Operational Availability (Ao): The probability that the system will be ready to perform its specified function, in its specified and intended operational environment, when called for at a random point in time.

Part: One piece or two or more pieces joined together which are not normally subject to disassembly without destruction of designed use.

Performance: A quantitative measure characterizing a physical or functional attribute relating to execution of an operation or function. Performance attributes include quantity (how many and how much), quality (how well), coverage (how much area, how far), timeliness (how responsive, how frequent), and readiness (availability, mission/operational readiness). Performance is an attribute for all systems, people, products, and processes including those for development, production, verification, deployment, operations, support, training, and disposal. Thus supportability parameters, manufacturing process variability, reliability and so forth, are all performance measures.

Physical Configuration Audit (PCA): The formal examination of the "as-built" configuration of a configuration item against its technical documentation to establish or verify the configuration item's product baseline.

Positive Control (During Flight): The ability to reduce to an acceptable level, the hazards associated with the errant flight of a launch vehicle during test and operations; normally achieved with a flight or thrust termination system.

Primitive Data: Is data that can be directly observed, such as the program size (i.e., Lines of Code), number of defects observed in unit testing, or total development time for the project.

Process Characterization: An activity that: (1) Identifies the key inputs and outputs of a process; (2) Collects data on their behavior over the entire operating range; (3) Estimates the steady-state behavior at optimal operating conditions; and (4) Builds models describing the parameter relationships across the operating range.

Product: Anything that is used or produced to satisfy a need (e.g., facilities, systems, hardware, software, firmware, data, processes, materials, or services).

Product Baseline: The initially approved documentation describing all necessary functional and physical characteristics of the configuration item (CI); any required joint and combined operations; selected functional and physical characteristics designated for production acceptance testing; and tests necessary for deployment/installation, support, training, and disposal of the CI. This baseline is usually initiated at the Critical Design Review (CDR) and finalized at the Physical Configuration Audit (PCA), and normally includes product, process, and material specifications, engineering drawings, and other related data.

Provisions: The 14 key individual focus areas included in this document. The detailed requirements are listed in each of the provisions.

Qualification Test: These tests simulate defined environmental conditions with a predetermined safety factor (margin), the results indicating whether a given design can perform its function within the expected mission environment for the system. These tests are performed on items that are representative of their expected fielded configuration.

Quality: (1) The composite of materiel attributes including performance features and characteristics of a production or service to satisfy a customer's given need. (2) The characteristics of a product or service that bear on its ability to satisfy stated or implied needs.

Quality Assurance (QA): A planned and systematic pattern of all actions necessary to provide confidence that adequate technical requirements are established, that products and services conform to established technical requirements, and that satisfactory performance is achieved.

Quality Record: A document recording specific information or data that relates to a procedure, process, or work instruction. Quality records are proof or objective evidence that an organization is complying with its procedures, practices, standards, and policies.

Relevant Failure: A product (or service) failure that has been verified and can be expected to occur in normal operational use. Relevancy indicates whether a specific failure should "count" or not in the calculation of reliability for a product or service.

Reliability: The probability that a system or subsystem will perform its intended function failure free for a specified interval under stated conditions or stated environments.

Repair: A procedure which reduces, but not completely eliminates, a nonconformance and which has been reviewed and concurred in by the Material Review Board (MRB) and approved for use by the Government. The purpose of repair is to reduce the effect of the nonconformance. Repair is distinguished from rework in that the characteristic after repair still does not completely conform to the applicable drawings, specifications, or contract requirements. Except for standard repair procedures, proposed repairs approved by the Government are authorized for use on a one time basis only.

Residual Safety Risk: The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, IAW the system safety design order of precedence.

Rework: A procedure applied to a nonconformance that will completely eliminate it and result in a characteristic that conforms completely to drawings, specifications, or contract requirements. Rework does not require Government approval.

Risk: A measure of the inability to achieve program objectives within defined cost and schedule constraints. Risk is associated with all aspects of the program (e.g., threat, technology, design processes, or work breakdown structure elements). It has two components, likelihood of failing to achieve a particular outcome, and consequences of failing to achieve that outcome.

Risk Analysis: A detailed examination of each identified program risk, which refines the description of the risk, isolates the cause, and determines the impact of the program risk in terms of its probability of occurrence, its consequences, and its relationship to other risk areas or processes.

Risk Identification: The process of examining the program areas and each critical technical process to identify and document the associated risk.

Risk Management: The act or practice of dealing with risk. It includes planning for risk, assessing (identifying and analyzing) risk areas, developing risk handling options, monitoring risks to determine how risks have changed, and documenting the overall risk management program. It includes plans and actions taken to identify, assess, mitigate, continuously track, control, and document program risks.

Risk Mitigation: (1) The process of avoiding, reducing and controlling, transferring, or deliberately accepting risk on the program. (2) A plan to minimize the impact or likelihood of the risk. (3) A plan to reduce, avoid, or eliminate risk.

Risk Monitoring: A process that systematically tracks and evaluates performance of risk items against established metrics throughout the acquisition and deployment processes and develops further risk reduction handling options, as appropriate.

Safety Alerts: A notification to the operator that the system has entered an unsafe state and operator acknowledgement or other action is required.

Safety Critical: A term applied to a condition, event, operation, process, or item whose proper recognition, control, sequencing, performance, or tolerance is essential for safe system operation or use.

Safety Critical Function: A function whose proper recognition, control, sequencing, performance, or tolerance is essential for safe system operation or use.

Safety Critical Item: Any component whose failure or improper function would render the system less than dual fault tolerant for catastrophic or critical severity hazards.

Safety Critical Software: A condition, event, operation, process, or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use. Safety Critical Software includes firmware and software programs or routines where incorrect, inadvertent or improper functioning, functioning in an improper sequence, or failure to function when required can result in a hazard, loss of predictability, or control of the system.

Safety Inhibit: Any system design feature whose intended purpose is to eliminate a hazard or reduce the risk associated with the hazard by lessening the severity or lowering the likelihood that a mishap will occur.

Safety Kernel: An independent computer program that monitors the state of the system to determine when potentially unsafe system states occur and to return the system to a known safe state.

Software: The instructions and data which have been manually or automatically generated for use on a processor. While software may reside in volatile or non-volatile memory, for the purpose of this document, it does not include tools and instructions used in development of electronic devices.

Software Adequacy: The quantifiable ability of software to meet approved software and interface requirements.

Software Assurance: The planned and systematic set of activities that ensures that software life cycle processes and products conform to requirements, standards, and procedures.

Software Dependability: Trustworthiness of a computer system such that reliance can be justifiably placed on the service it delivers. Reliability, availability, and maintainability are aspects of dependability.

Software Product: The set of computer programs, procedures, and possibly associated documentation and data.

Software Quality: The ability of software to satisfy its specified requirements.

Software Quality Assurance: (1) A planned and systematic pattern of all actions necessary to provide adequate confidence that a software work product conforms to established technical requirements. (2) A set of activities designed to evaluate the process by which software work products are developed and maintained.

Software Reliability: (1) The probability that software will not cause failure of a system for a specified time under specified conditions. (2) The ability of a program to perform a required function under stated conditions for a stated period of time.

Note: For definition (1), the probability is a function of the inputs to and use of the system, as well as a function of the existence of faults in the software. The inputs to the system determine whether existing faults, if any, are encountered (IEEE 1633, Recommended Practices on Software Reliability).

Software Reuse: The process of implementing or updating software systems using existing software assets.

Standard Repair Procedure: A documented technique for repair of a type of nonconformance which has been demonstrated to be an adequate and cost effective method for repair when properly applied. Standard Repair Procedures are developed by the contractor, reviewed and concurred in by the Material Review Board, and approved by the Government for recurrent use under defined conditions. Defined conditions shall include an expiration date or a finite limit on the number of applications, or both.

Strong Data Typing: A fault tolerance technique wherein a discrete or variable data is represented by a bit pattern that is unique for each valid value and cannot be confused with any other valid value even as a result of a one or two bit error.

Subassembly: Two or more parts which form a portion of an assembly or a unit replaceable as a whole, but having a part or parts which are individually replaceable.

Subsystem: A functional grouping of components that combine to perform a major function within an element, such as attitude control and propulsion.

Supplier: An entity that provides a product or service. The term supplier also encompasses subcontractors and vendors.

System: (1) The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function with specified results, such as the gathering of specified data, its processing, and delivery to users. (2) A combination of two or more interrelated pieces of equipment (or sets) arranged in a functional package to perform an operational function or to satisfy a requirement.

System Loss: Within the context of this document, system loss does not refer to unavailability of a system; rather, it implies significant rework required or replacement is required to return the system to its undamaged state.

Technical Data Package: A technical description of an item adequate for supporting an acquisition strategy, production, engineering, and logistics support. The description defines the required design configuration and procedures required to ensure adequacy of item performance. It consists of all applicable technical data such as drawings and associated lists, specifications, standards, performance requirements, quality assurance provisions, and packaging details. Software and firmware may refer to Version Description Document or Software Version Description as the technical data package.

Test-Like-You-Fly: Operability validation approach that examines all applicable mission characteristics and determines the fullest practical extent to which those characteristics can be applied in testing. The "fullest practical extent" identifies physical and engineering limitations, and balances what can be done in a flight-like manner with acceptable and understood risk, and program constraints.

Unit: (1) An assembly or any combination of parts, subassemblies, and assemblies mounted together, normally capable of independent operation in a variety of situations. (2) A separately testable element specified in the design of a computer software component. (3) A logically separable part of a computer program.

Unsafe State: A system state that may result in a hazard/mishap.

Use-As-Is: A disposition of material with one or more minor nonconformances determined to be usable for its intended purpose in its existing condition.

Unverified Failure: Any failure for which, at the conclusion of the failure investigation, the root cause cannot be determined conclusively.

Validation: (1) Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. (2) The process of determining the degree to which a model and its associated data are an accurate representation of the real world from the perspective of the intended uses of the model.

Variance (Deviation or Waiver): A specific written authorization to depart from a particular requirement of a product's current approved configuration documentation for a specific number of units or a specified time period. (A variance differs from an engineering change in that an approved engineering change

requires corresponding revision of the product's current approved configuration documentation, whereas a variance does not).

Verification: (1) The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. (2) For Models and Simulation. The process of determining that a model implementation and its associated data accurately represent the conceptual description and specifications.

Version: (1) One of several sequentially created configurations of a data product. (2) A supplementary identifier used to distinguish a changed body or set of computer based data (software) from the previous configuration with the same primary identifier. Version identifiers are usually associated with data (e.g., files, databases, and software) used by, or maintained in, computers.